IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patentee: Jacobson

Patent No.: 7,231,668

Application No. 10/815,092

Issued: 12 June 2007

Title: NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM

Attorney Ref. No.: 065426.0002

Examiner: N. Wright

Art Unit: 2134

PETITION FOR ACCEPTANCE OF UNINTENTIONALLY DELAYED CLAIM FOR PRIORITY

Mail Stop Petition
Commissioner of Patents
Post Office Box 1450
Alexandria, Virginia 22313 1450

Dear Sir:

Applicant respectfully requests the Office grant this Petition for acceptance of an unintentionally delayed claim for priority. In support of her Petition, Applicant states as follows:

On 12 June 2007, U.S. Patent No. 7,231,668 ("the '668 Patent") issued. The '668 Patent issued on U.S. Patent Application No. 10/815,092 ("the '092 Application"), which was filed on 31 March 2004. Counsel of record at the time of the filing of the '092 Application was MOORE, HANSEN & SUMNER of Minneapolis, Minnesota. As part of the

filing of the '092 Application, MOORE, HANSEN & SUMNER included a Utility Patent Application Transmittal (attached hereto as Exhibit A), which indicated that the '092 Application is a Continuation Application of U.S. Patent Application No. 09/104,946 ("the '946 Application), and, consequently, claims priority thereto. The '946 Application was filed on 25 June 1998 by MERCHANT, GOULD, SMITH, EDELL, WELTER & SCHMIDT, also of Minneapolis, Minnesota.

Additionally indicated on the Utility Patent Application Transmittal was the notation that the Declaration of Inventorship was that from the '946 Application. A copy of the Declaration was also included with the initial filing of the '092 Application. This copy is attached hereto as Exhibit B.

Finally, also included with the initial filing of the '092 Application, MOORE, HANSEN & SUMNER provided a Preliminary Amendment, in which the Office was requested to "amend the attached new continuation application as follows." This Preliminary Amendment is attached hereto as Exhibit C.

Counsel of record for the '092 Application then proceeded to LEFEVOUR LAW GROUP, LLC of Western Springs, Illinois on 15 March 2006. On 24 March 2006, the Office issued an Office Communication, in which it established a Statutory Double Patenting Rejection, based on the '946 Application, which had, by then, issued as U.S. Patent No. 6,735,701 ("the '701 Patent"). A copy of the 24 March 2006 Office Communication is attached hereto as Exhibit D.

Applicant's current counsel ascended to counsel of record on 12 September 2006. From the time that Applicant's current counsel became counsel of record in the '092 Application until the issuance of the '668 Patent, each time Applicant's current

counsel reviewed the Private PAIR system on the Office's Web page, the Image File Wrapper maintained by the PAIR system indicated that the '092 Application maintained a claim for priority, as a Continuation, to the '701 Patent. *See, e.g.*, Bibliographic Data Sheets from 24 March 2006 and 10 October 2006, collectively attached hereto as Exhibit E.

Upon receiving and reviewing the '668 Patent, it was realized that the claim for priority was not indicated on the face of the '668 Patent. Consequently, on 23 October 2007, Applicant requested a Certificate of Correction be entered in the '668 Patent, indicating the claim for priority. A copy of the Certificate of Correction Request is attached hereto as Exhibit F.

This request was denied on 27 December 2007. In the Denial, it was stated that "[a]n amendment containing a specific reference to the earlier filed application has not been submitted nor was such a reference submitted during the pendency of the application." Further, the Office indicated that "[a] grantable petition to accept [an unintentional] claim for benefit of the prior application must be filed, including surcharge 37 CFR 1.17(e). A copy of this Denial is attached hereto as Exhibit G.

Unfortunately, Applicant's counsel of record did not receive the Notice of denial of the Certificate of Correction through the U.S. Postal Service. Rather, upon its regular Six (6) Month status check, which included a search of the PAIR system on the USPTO Web Page, Applicant's counsel of record downloaded the Denial on or around 23 April 2008.

Upon receiving the Denial, Applicant's counsel of record immediately undertook a review of the file history of the '092 Application to determine what exactly occurred,

given the fact that Applicant's counsel of record was not counsel of record throughout the prosecution of the '092 Application. As a result of Applicant's counsel's investigation, it has since come to the attention of Applicant's counsel of record that, although previous counsel of record indicated on the Utility Patent Transmittal Form (Exhibit A), that the '092 Application claims priority, as a Continuation, to what would eventually become the '701 Patent, a specific claim for priority in the '092 Application was unintentionally omitted.

Consequently, Applicant respectfully requests that the above-captioned U.S. Patent be amended to indicate that it is a Continuation Application, claiming priority to U.S. Patent No. 6,735,701. A copy of the '701 Patent is attached hereto as Exhibit H. Additionally, Applicant states that the entire delay between the time the claim for priority was due and today's date (*i.e.*, the date this Petition is filed) is unintentional.

Further, Applicant understands that a surcharge under 37 CFR 1.17(t) is required with this Petition. This Fee may be charged to Deposit Account No. 042223. Further, any other fees relating to this Petition may also be charged to Deposit Account No. 042223.

Please contact the undersigned Patentee's Attorney Of Record if there are any questions.

Respectfully submitted,

Date: 22 July 2008

/ Timothy M. Morella /

Timothy M. Morella
Reg. No. 45,277

DYKEMA GOSSETT PLLC
Ten South Wacker Drive
Chicago, Illinois 60606 7453
312 627 2592 (Voice)
312 627 2302 (Facsimile)

CHICAGO\2475697.1
ID\TMMO

Exhibit A

UTILITY PATENT APPLICATION TRANSMITTAL (New Nonprovisional Applications Under 37 CFR § 1.53(b))	Atty. Docket No. M61-002-04-US Atty. Customer No. 22854

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Transmitted herewith is the patent application of ( ) application identifier or (X) first named inventor, Andrea Jacobson, entitled NETWORK POLICY AND MANAGEMENT AND EFFECTIVENESS SYSTEM, for a(n):

17510 U.S.PTO
10/815092
033104

( ) Original Patent Application.

(X) Continuing Application (prior application not abandoned):
- (X) Continuation ( ) Divisional ( ) Continuation-in-part (CIP) of prior application No: 09/104,946 Filed on: June 25, 1998.
- (X) A statement claiming priority under 35 USC § 120 has been added to the specification.

Enclosed are:
- ( ) Specification; __ Total Pages. ( ) Drawing(s); __ Total Sheets.
- ( ) Oath or Declaration:
  - ( ) A Newly Executed Combined Declaration and Power of Attorney:
    - ( ) Signed. ( ) Unsigned. ( ) Partially Signed.
  - (X) A Copy from a Prior Application for Continuation/Divisional (37 CFR § 1.63(d)).
    - (X) Incorporation by Reference. The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied, is considered as being part of the disclosure of the accompanying application and is hereby incorporated herein by reference.
    - ( ) Signed Statement Deleting Inventor(s) Named in the Prior Application. (37 CFR § 163(d)(2)).
- ( ) Power of Attorney. (X) Return Receipt Postcard.
- ( ) Associate Power of Attorney. (X) A Check in the amount of $ 385 for the Filing Fee.
- ( ) Preliminary Amendment. ( ) Information Disclosure Statement and Form PTO-1449.
- ( ) A Duplicate Copy of this Form for Processing Fee Against Deposit Account..
- ( ) A Certified Copy of Priority Documents (if foreign priority is claimed).
- (X) Applicant claims small entity status.
- ( ) Other: _____

CLAIMS AS FILED				
FOR	NO. FILED	NO. EXTRA	RATE	FEE
Total Claims	1	0	$9.00	$ 0.00
Independent Claims	1	0	$43.00	$ 0.00
Multiple Dependent Claims (if applicable)				$0.00
Basic Filing Fee				$385.00
Total Filing Fee				$ 385.00

Charge $_____ to Deposit Account 13-4300 pursuant to 37 CFR § 1.25. At any time during the pendency of this application, please charge any fees required or credit any overpayment to this Deposit Account.

Respectfully submitted,

By: _____
Allen J. Oh
Attorney of Record, Reg. No. 42,047

Date: March 31, 2004

Correspondence Address:

Moore, Hansen & Sumner
2900 Wells Fargo Center 90 South Seventh Street
Minneapolis, MN 55402
Phone: 612-332-8200
Fax: 612-332-1780

I hereby certify that this is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated below and is addressed to:

Commissioner for Patents
Alexandria, VA 22313-1450

By: _____
Typed Name: Nichole Williams

Express Mail Label No.: EL495653023US

Date of Deposit: March 31, 2004

Exhibit B

M&G 12369.1US01

MERCHANT, GOULD, SMITH, EDELL, WELTER & SCHMIDT

United States Patent Application

DECLARATION UNDER 37 C.F.R. § 1.63

As a below named inventor I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM

The specification of which
a. ☐ is attached hereto
b. ☒ is entitled NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM, having an attorney docket number 12369.1US01
c. ☐ was filed on as application serial no. and was amended on (if applicable) (in the case of a PCT-filed application) described and claimed in international no. filed and as amended on (if any), which I have reviewed and for which I solicit a United States patent.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56 (attached hereto).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on the basis of which priority is claimed:

a. ☒ no such applications have been filed.
b. ☐ such applications have been filed as follows:

FOREIGN APPLICATION(S), IF ANY, CLAIMING PRIORITY UNDER 35 USC § 119			
COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)
ALL FOREIGN APPLICATION(S), IF ANY, FILED BEFORE THE PRIORITY APPLICATION(S)			
COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)

I hereby claim the benefit under Title 35, United States Code, § 120/365 of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. APPLICATION NUMBER	DATE OF FILING (day, month, year)	STATUS (patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

U.S. PROVISIONAL APPLICATION NUMBER	DATE OF FILING (Day, Month, Year)

I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/ organization who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Merchant, Gould, Smith, Edell, Welter & Schmidt to the contrary.

Please direct all correspondence in this case to Merchant, Gould, Smith, Edell, Welter & Schmidt at the address indicated below:

Merchant, Gould, Smith, Edell,
Welter & Schmidt
3100 Norwest Center
90 South Seventh Street
Minneapolis, MN 55402-4131

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2	Full Name Of Inventor	Family Name JACOBSON	First Given Name ANDREA	Second Given Name M.
0	Residence & Citizenship	City ST. PAUL	State or Foreign Country MINNESOTA	Country of Citizenship USA
1	Post Office Address	Post Office Address 250 EAST SIXTH STREET, #610	City ST. PAUL	State & Zip Code/Country MINNESOTA 55101/USA
Signature of Inventor 201: *Jacobson*			Date: 6/25/98	
2	Full Name Of Inventor	Family Name	First Given Name	Second Given Name
0	Residence & Citizenship	City	State or Foreign Country	Country of Citizenship
2	Post Office Address	Post Office Address	City	State & Zip Code/Country
Signature of Inventor 202:			Date:	
2	Full Name Of Inventor	Family Name	First Given Name	Second Given Name
0	Residence & Citizenship	City	State or Foreign Country	Country of Citizenship
3	Post Office Address	Post Office Address	City	State & Zip Code/Country
Signature of Inventor 203:			Date:	
2	Full Name Of Inventor	Family Name	First Given Name	Second Given Name
0	Residence & Citizenship	City	State or Foreign Country	Country of Citizenship
4	Post Office Address	Post Office Address	City	State & Zip Code/Country
Signature of Inventor 204:			Date:	

2	Full Name Of Inventor	Family Name	First Given Name	Second Given Name
0	Residence & Citizenship	City	State or Foreign Country	Country of Citizenship
5	Post Office Address	Post Office Address	City	State & Zip Code/Country
Signature of Inventor 205:			Date:	

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)–(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden–of–proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application:

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

Exhibit C

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Minneapolis, Minnesota
March 31, 2004

Applicant: Jacobson

Serial No.: Unknown

Filed: Herewith

For: **NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM**

Atty. Docket No.: M61-002-04-US

PRELIMINARY AMENDMENT

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madam:

Please amend the attached new continuation application as follows:

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. 1.10)

Express Mail Label No. EL495653023US Date of Deposit: March 31, 2004

I hereby certify that this correspondence is, on the date shown above, being deposited with the United States Postal Service "Express Mail " Service under 37 CFR 1.10, in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Nichole Williams
Print Name of Person Mailing Correspondence

[Signature]

IN THE CLAIMS

Amendments to the Claims

1. (Previously Amended) A method for dynamically assisting a system administrator of a computer network in upgrading compliance policy based on behavior of system users; the method comprising the steps of:

storing in a database a plurality of compliance policy opti9ons;

developing an initial compliance policy option potentially applicable to network users;

automatically evaluating over time the appropriateness of the initial compliance policy option based on the potentially evolving compliance history of users;

automatically compiling and providing to the system administrator over time a dynamic knowledge base comprising automated network user policy compliance violation documentation;

automatically determining from the knowledge base policy compliance violation documentation that the initial compliance policy option is ineffective;

automatically selecting from the database and recommending to the system administrator an alternate compliance policy options; and

automatically requesting that the system administrator confirm the change to the alternate compliance policy option

whereby compliance policy options are dynamically altered and provided to the system administrator in order to eliminate ineffective compliance policy options

Please cancel Claims 2-12.

REMARKS

Claim 1 remains in this application. Claims 2-12 have been cancelled or withdrawn.

Conclusion

On the basis of the foregoing amendments, remarks, and papers of record, Applicant respectfully submits that the remaining claim 1 is in condition for allowance. Applicant respectfully requests a Notice of Allowance.

Respectfully submitted,
Andrea-Marie Jacobson
By her attorneys

MOORE, HANSEN & SUMNER PLLP
2900 Wells Fargo Center
90 South Seventh Street
Minneapolis, Minnesota 55402
(612) 332-8200

Date: March 31, 2004

By _____
Allen J. Oh, Registration No. 42,047

Exhibit D

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,092	03/31/2004	Andrea M. Jacobson		7333

50717 7590 03/24/2006

LEFEVOUR LAW GROUP, LLC
4365 LAWN AVE
SUITE 5
WESTERN SPRINGS, IL 60558

EXAMINER	
WRIGHT, NORMAN M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/815,092	JACOBSON, ANDREA M.	
	Examiner	Art Unit	
	Norman M. Wright	2134	

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1* is/are pending in the application.

4a) Of the above claim(s) *2-12* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The reply filed on 3/31/2004, as a preliminary amendment, canceling claims 2-12 is acknowledged. The sole outstanding claim is now claim 1.

Double Patenting

2. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

3. Claim1 is rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 1 of prior U.S. Patent No. 6,735701. This is a double patenting rejection.

As to claim 1, it is appears to claim identical subject matter with the same scope. Accordingly, it is rejected as a statutory double patenting rejection.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Norman M. Wright whose telephone number is (571) 272-3844. The examiner can normally be reached on weekdays, from 8AM to 4 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Norman M. Wright
Primary Examiner
Art Unit 2134

Exhibit E

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 7333

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/815,092	03/31/2004 RULE	726	2134	

APPLICANTS

Andrea M. Jacobson, St. Paul, MN;

** CONTINUING DATA **********

This application is a CON of 09/104,946 06/25/1998 PAT 6,735,701

** FOREIGN APPLICATIONS **********

N/A

IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** SMALL ENTITY **
** 06/10/2004

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no	MN	51	1	1
35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged Examiner's Signature Initials				

ADDRESS
50717
LEFEVOUR LAW GROUP, LLC
4365 LAWN AVE
SUITE 5
WESTERN SPRINGS , IL
60558

TITLE
Network policy management and effectiveness system

FILING FEE	FEES: Authority has been given in Paper	☐ All Fees
RECEIVED 385	No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ 1.16 Fees (Filing)
		☐ 1.17 Fees (Processing Ext. of time)
		☐ 1.18 Fees (Issue)


Other
Credit

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 7333

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/815,092	03/31/2004 RULE	726	2134	065426.0002

APPLICANTS

Andrea M. Jacobson, St. Paul, MN;

**** CONTINUING DATA ***************************

This application is a CON of 09/104,946 06/25/1998 PAT 6,735,701

**** FOREIGN APPLICATIONS ********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** SMALL ENTITY **
** 06/10/2004

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no 35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance Verified and Acknowledged _____ Examiner's Signature Initials	MN	51	1	1

ADDRESS
50717

TITLE

Network policy management and effectiveness system

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:
385	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Exhibit F

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patentee: Jacobson

Patent No.: 7,231,668

Application No. 10/815,092

Issued: 12 June 2007

Title: NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM

Attorney Ref. No.: 065426.0002

Examiner: N. Wright

Art Unit: 2134

CERTIFICATE OF CORRECTION

Commissioner of Patents
Post Office Box 1450
Alexandria, Virginia 22313 1450

Dear Sir:

Upon a review of the above-referenced U.S. Patent, it was determined that at least one mistake was made during the printing of the Patent by the U.S. Patent and Trademark Office. The mistake listed herein was made by the Office and through no fault of the Patentee. Therefore, it is believed that no fees are required. Please contact the undersigned Patentee's Attorney Of Record if there are any questions.

Pursuant to 35 U.S.C. § 254 and 37 C.F.R. § 1.322, request is made to correct the Patent Cover Sheet of Issued U.S. Patent No. 7,231,668, which issued on 12 June 2007.

As set forth in the attached PTO Form PTO-1050, the following corrections are requested:

- The Patent Cover Sheet should include a heading entitled "Related U.S. Application Data";
- Under this heading, the following statement should be inserted: -- Continuation of application No. 09/104,946, filed on June 25, 1998, now Pat. No. 6,735,701. --.

In support of this Request, enclosed is a copy of the U.S. Patent Publication document relating to the above-referenced Patent, bearing the above-cited information under the heading "Related U.S. Application Data."

Please correct the Cover Sheet of the Patent and forward a copy to my attention.

Respectfully submitted,

Date: 23 October 2007

/ Timothy M. Morella /

Timothy M. Morella
Reg. No. 45,277

DYKEMA GOSSETT PLLC
Ten South Wacker Drive
Chicago, Illinois 60606 7453
312 627 2592 (Voice)
312 627 2302 (Facsimile)

CHICAGO\2388979.1
ID\TMMO

PTO/SB/44 (09-07)
Approved for use through 08/31/2010. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,231,668

APPLICATION NO.: 10/815,092

ISSUE DATE : 12 June 2007

INVENTOR(S) : Andrea M. Jacobson

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

The Cover Sheet of the above-referenced U.S. Patent should include a heading entitled:

-- Related U.S. Application Data --.

Further, the following language should be inserted below the aforementioned heading:

-- Continuation of application No. 09/104,946, filed on 25 June 1998, now Pat No. 6,735,701. --.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Timothy M. Morella, Dykema Gossett PLLC, Ten South Wacker Drive, Chicago, Illinois, 60606.7453

Exhibit G

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

12/27/07

Patent No. : 7231668 B2
Ser. No. : 10/815092
Inventor(s) : Jacobson
Issued : June 12, 2007
Title : **NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM**
Docket No. : 065426.0002

Re: Request for Certificate of Correction

Consideration has been given your request for the issuance of a certificate of correction for the above-identified patent.

An amendment containing a specific reference to the earlier filed application has not been submitted nor was such a reference submitted during the pendency of the application.

A grantable petition to accept on unintentionally claim for benefit of the prior application must be filed, including surcharge 37 CFR 1.17 (e).

In view of the foregoing, your request is hereby **denied**.

Elisha Evans
For Cecelia Newman, Supervisor
Decisions & Certificates
of Correction Branch
(703) 308-9390 ext. 110

DYKEMA GOSSETT PLLC
10 S. WACKER DR., STE. 2300
CHICAGO IL 60606

CBN/eme

Exhibit H

US006735701B1

(12) **United States Patent**
Jacobson

(10) **Patent No.: US 6,735,701 B1**
(45) **Date of Patent: May 11, 2004**

(54) **NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM**

(75) Inventor: **Andrea M. Jacobson**, St. Paul, MN (US)

(73) Assignee: **MacArthur Investments, LLC**, Edina, MN (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/104,946**

(22) Filed: **Jun. 25, 1998**

(51) **Int. Cl.**[7] **C06F 11/30**
(52) **U.S. Cl.** **713/201**; 713/202; 713/200
(58) **Field of Search** 713/200–202

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,142,612	A *	8/1992	Skeirik	395/11
5,197,114	A *	3/1993	Skeirik	395/22
5,355,474	A *	10/1994	Thuraisngham et al.	395/600
5,408,586	A *	4/1995	Skeirik	395/23
5,440,744	A *	8/1995	Jacobson et al.	395/650
5,579,222	A *	11/1996	Bains et al.	395/712
5,603,054	A	2/1997	Theimer et al.	395/826
5,621,889	A *	4/1997	Lermuzeaux et al.	395/186
5,797,128	A *	8/1998	Birnbaum	707/5
5,845,065	A *	12/1998	Conte et al.	395/186
6,070,244	A *	5/2000	Orchier et al.	713/201

FOREIGN PATENT DOCUMENTS

WO	WO 93/11480	6/1993

OTHER PUBLICATIONS

"Data Exchange Executive," IBM TDB, Jul. 1993, vol. 36, Iss No. 7, p. 435–438; {IDB–ACC–No:NN9307435."

Grimm, R. et al., "Security policies in OSI–management experiences from the DeTeBerkom project BMSec", *Computer Networks and ISDN Systems*, vol. 28, No. 4, pp. 499–511 (Feb. 1996).

"SecureDelete—a utility to delete files securely", http://www.gammon.com.au/utilities/securedelete.htm (Sep. 14, 1998); 3 pgs.

"Review: Burn It", http://macworld.zdnet.com/pages/april.97/Reviews.3342.html (Sep. 14, 1998); 3 pgs.

"Content Advisor—Products Page", http://www.contentadvisor.com/products.products.html (Sep. 14, 1998); 1 pg.

"Content Advisor—Corporate Profile", http://www.contentadvisor.com/company/company.html (Sep. 14, 1998); 1 pg.

"SmartFilter—Tour, Monitoring and Control Features", http://www.sctc.com/P_Tool_SF_Tour_monandcont.html (Sep. 19, 1998); 1 pg.

"SF—Key Advantages", http://www.sctc.com/P_Tool_SF_Keys.html (Sep. 19, 1998); 2 pgs.

"SF—Requirements", http://www.sctc.com/P_Tool_SF_Regs.html (Sep. 19, 1998); 1 pg.

"Vendor's Guide to Software Pricing . . . ter Articles on License Management", http://www.globetrotter.com/ms_til.html (Apr. 7, 1998); 6 pgs.

"No Excuses Licensing", http://www.globetrotter.com/ecs1.htm (Feb. 3, 1998); 5 pgs.

"Seven Steps to Overcome Pricing Un . . . ter Articles on License Management", http://www.globetrotter.com/ms_2do.htm (Apr. 7, 1998) 2 pgs.

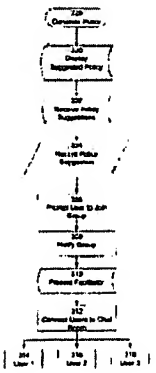
(List continued on next page.)

Primary Examiner—Norman M. Wright
(74) *Attorney, Agent, or Firm*—Moore, Hansen & Sumner

(57) **ABSTRACT**

A method, apparatus, and article of manufacture for maintaining policy compliance on a computer network is provided. The method provides the steps of electronically monitoring network user compliance with a network security policy stored in a database, electronically evaluating network security policy compliance based on network user compliance, and electronically undertaking a network policy compliance action in response to network security policy compliance.

12 Claims, 51 Drawing Sheets

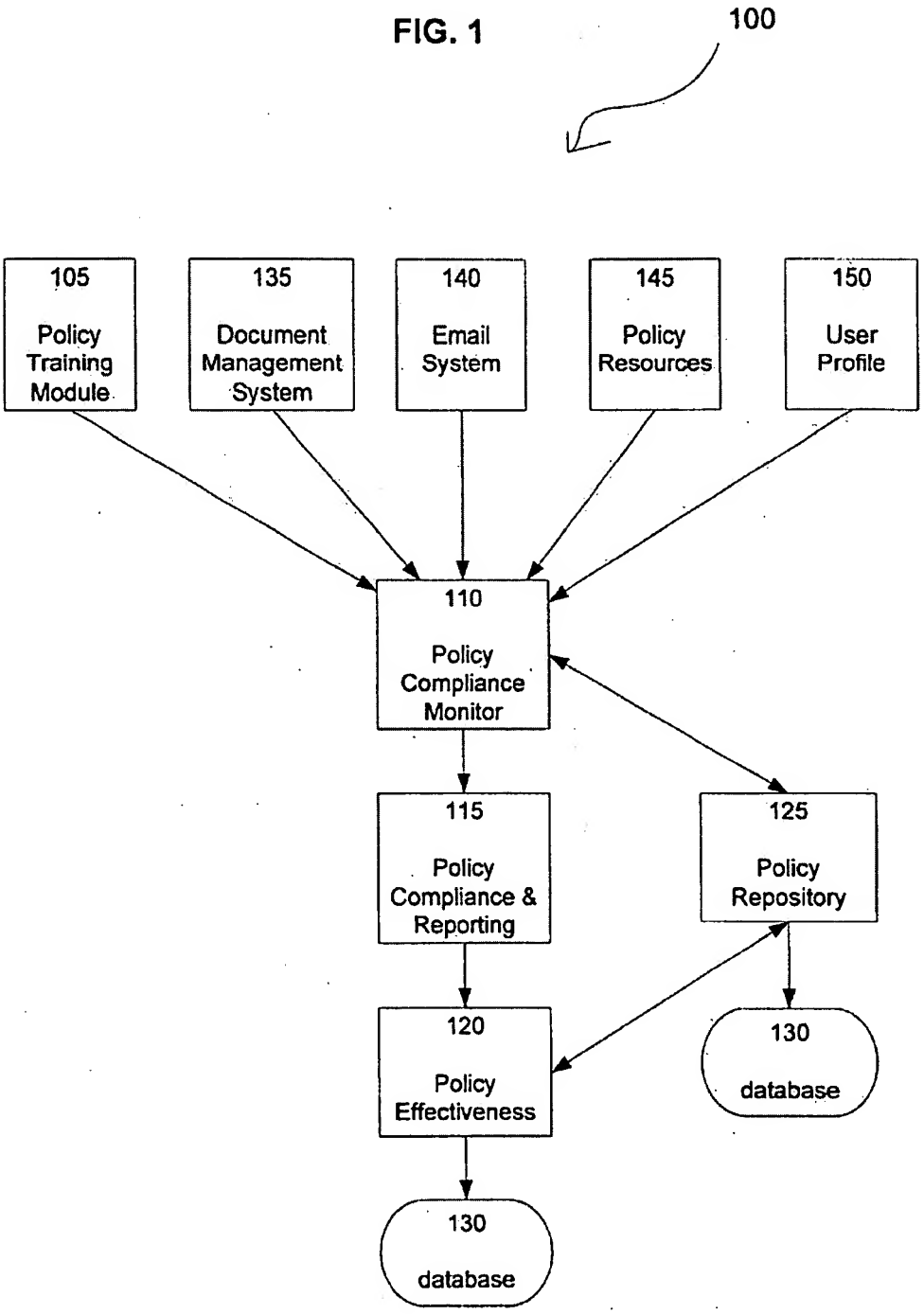


OTHER PUBLICATIONS

"Conceptual description of a generi . . . ter Articles on License Management", http://globetrotter.com/ms_lm.htm (May 18, 1998) 3 pgs.
"Press Release—Poulton Associates, Inc.", http://www.poulton.com/ispPR4-98.htm (Sep. 23, 1998), 2 pgs.
"ISPCweb—Poulton Associates, Inc.", http://www.poulton.com/ispcweb.htm (Sep. 23, 1998); 2 pgs.
"As courts increasingly hold firms . . . fast becoming a . . . legal necessity", http://www.drj.com/new2dr/w2_022.htm (Feb. 2, 1998); 5 pgs.
"Risk Analysis Techniques", http://www.drj.com/new2dr/w3_030.htm (Feb. 2, 1998); 8 pgs.
"White papers—Watermarking", http://www.dupont.com/Antron/mark.html (Jul. 16, 1998); 1 pg.
"About Digital Watermarks", http://www.digimarc.com/about_wm.html (Mar. 10, 1998); 4 pgs.
"Digimarc Corporate Series", http://www.digimarc.com/corp_solutions.html (Mar. 10, 1998); 3 pgs.
"Welcome to Digimarc", http://www.digimarc.com/ (Mar. 10, 1998); 2 pgs.
"MarcCentre", http://www.digimarc.com/marc_page.html (Mar. 10, 1998); 1 pg.
"Data Devices International—Tape Backup Procedures and Maintenance", http://www.datadev.com/tapebackup/tape-backup.htm (Sep. 9, 1998); 2pgs.
"Halebopp Backup Procedures", http://www.gb.nrao.edu/~cmyers/backup.html (Sep. 9, 1998); 2 pgs.
"ISSEL—Intra.doc! Management System", http://www.issel.co.uk/intradoc_ms.html (Feb. 23, 1998); 2 pgs.
"ISSEL—Intra.doc! Architecture", http://www.issel.co.uk/intradoc_architecture.html (Feb. 23, 1998); 2 pgs.
"Intra.doc! Product Suite", http://www.intranetsol.com/products/prodsuit.html (Feb. 23, 1998); 8 pgs.
"Intra.doc! Management System—Web . . . nagement and Enterprise Publishing", http://intranetsol.com/products/ms-broch.html (Feb. 23, 1998); 4 pgs.
"High-tech Manufacturer Gains Compe . . . With Web-based Document Management", http://www.intranet-sol.com/products/success/sshight.html (Feb. 23, 1998) 3 pgs.
"QRMS—Features", http://www.qrms.com/features.htm (Feb. 18, 1998); 19 pgs.
"The TPI Group Inc.—Software Asset Management", http://www.tpi-group.com/whitepapers/wpsasset.html (Feb. 3, 1998); 1 pg.
"The TPI Group—Software Asset Management in a Client Server Architecture", http://www.tpi-group.com/whitepapers/wpsasset.html (Feb. 3, 1998); 11 pgs.
Branscum, D., "bigbrother@the.office.com—Your boss can track every click you make.", *Newsweek*, Apr. 27, 1998, p. 78.
Fox, J., "Compensating your executive team on a shoestring", *Ventures*, Nov. 1997, pp. 14–16.
"Corel WordPerfect Suite 8—Data Formats Supported", White Paper, Aug. 1997 (p. 16).

* cited by examiner

FIG. 1



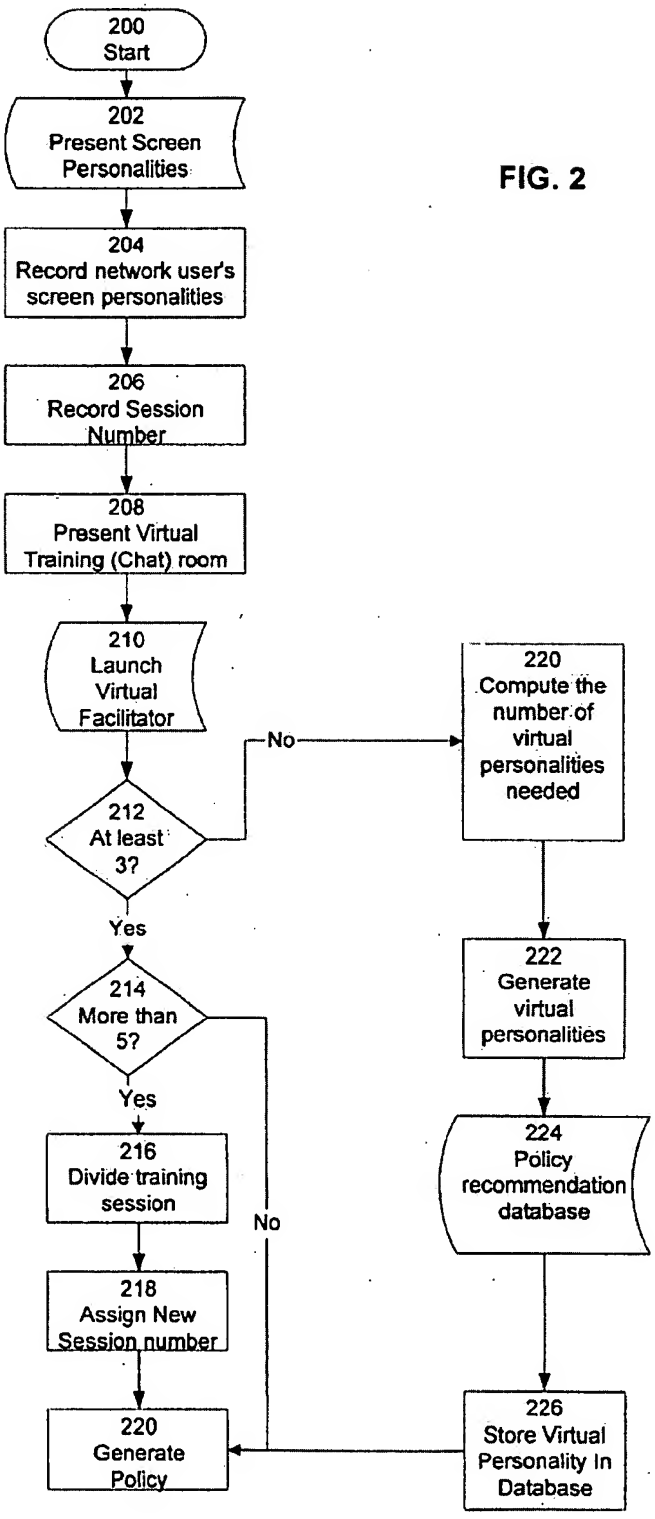


FIG. 2

FIG. 3A

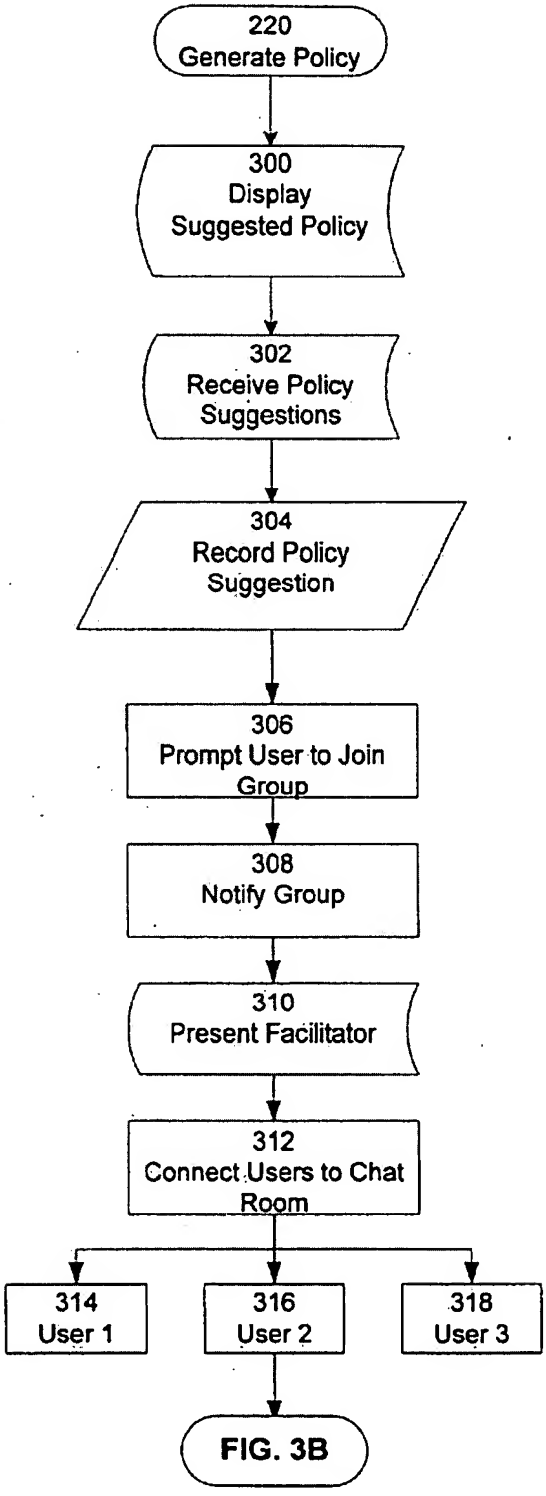


FIG. 3B

FIG. 3B

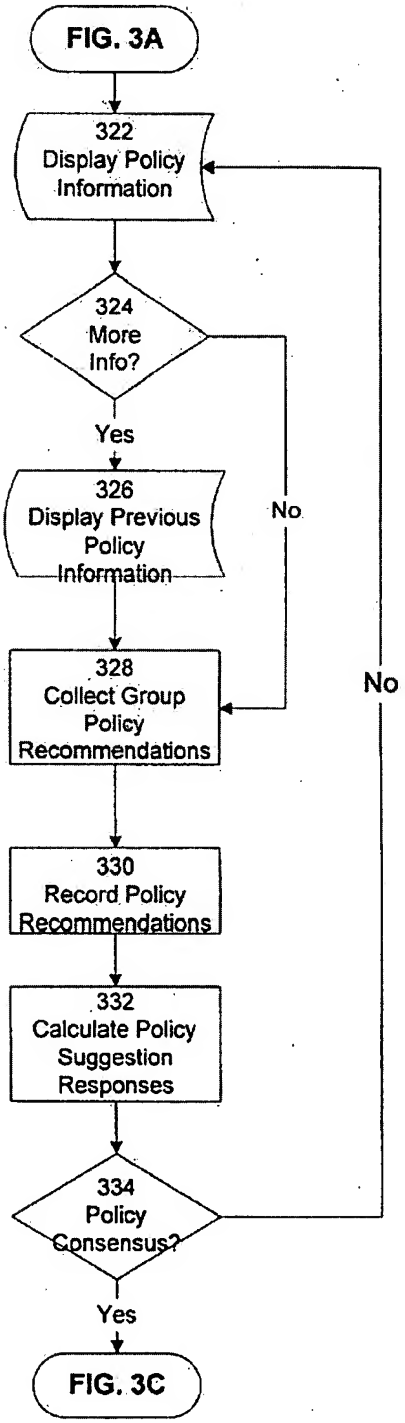


FIG. 3C

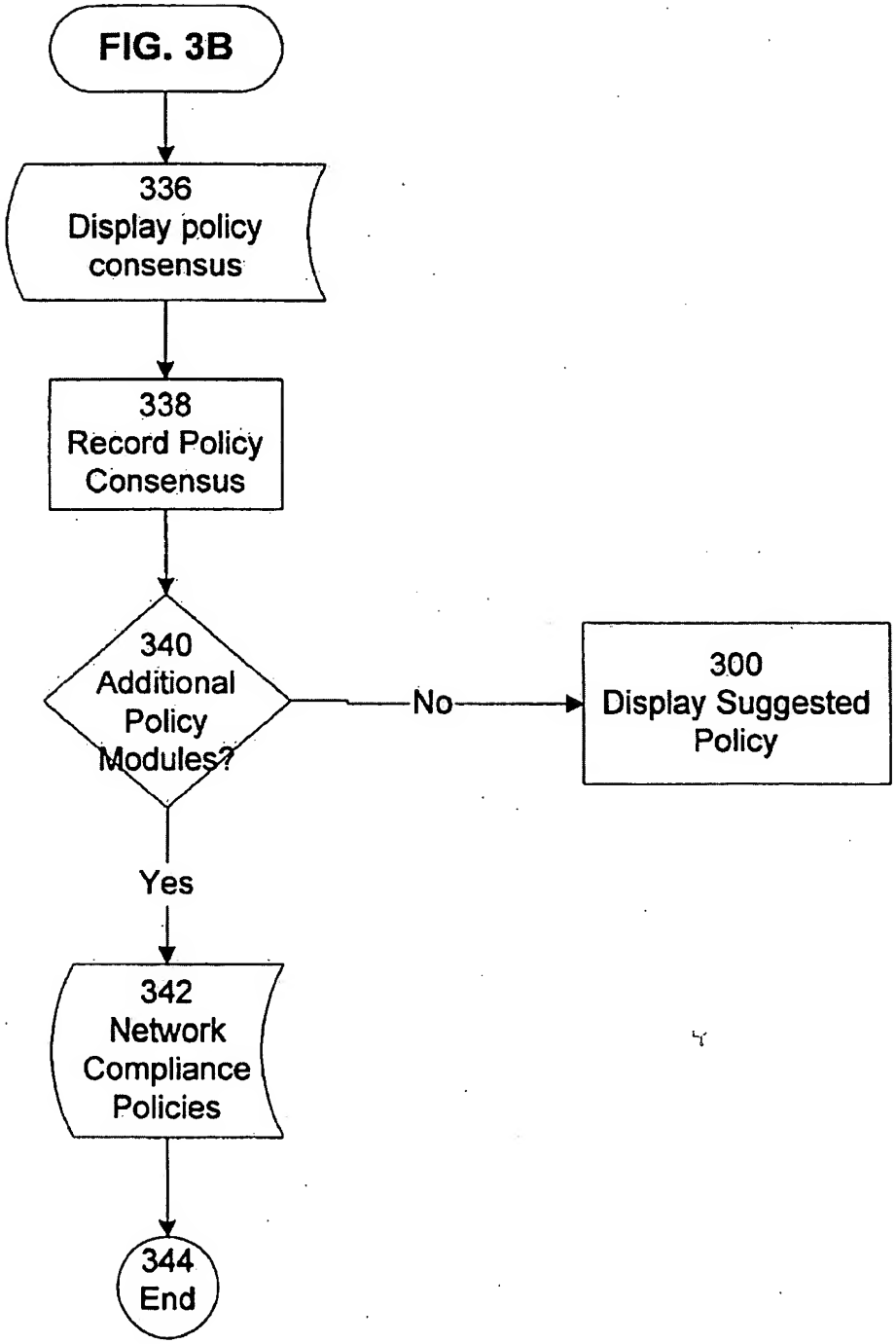


FIG. 4

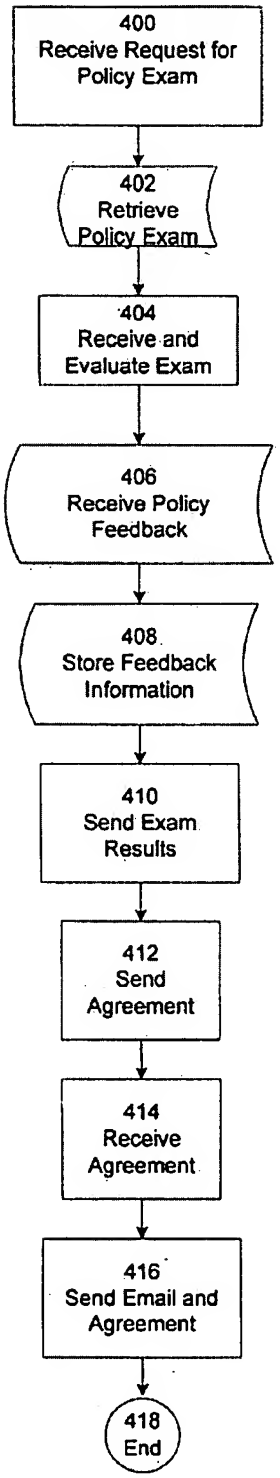


FIG. 5

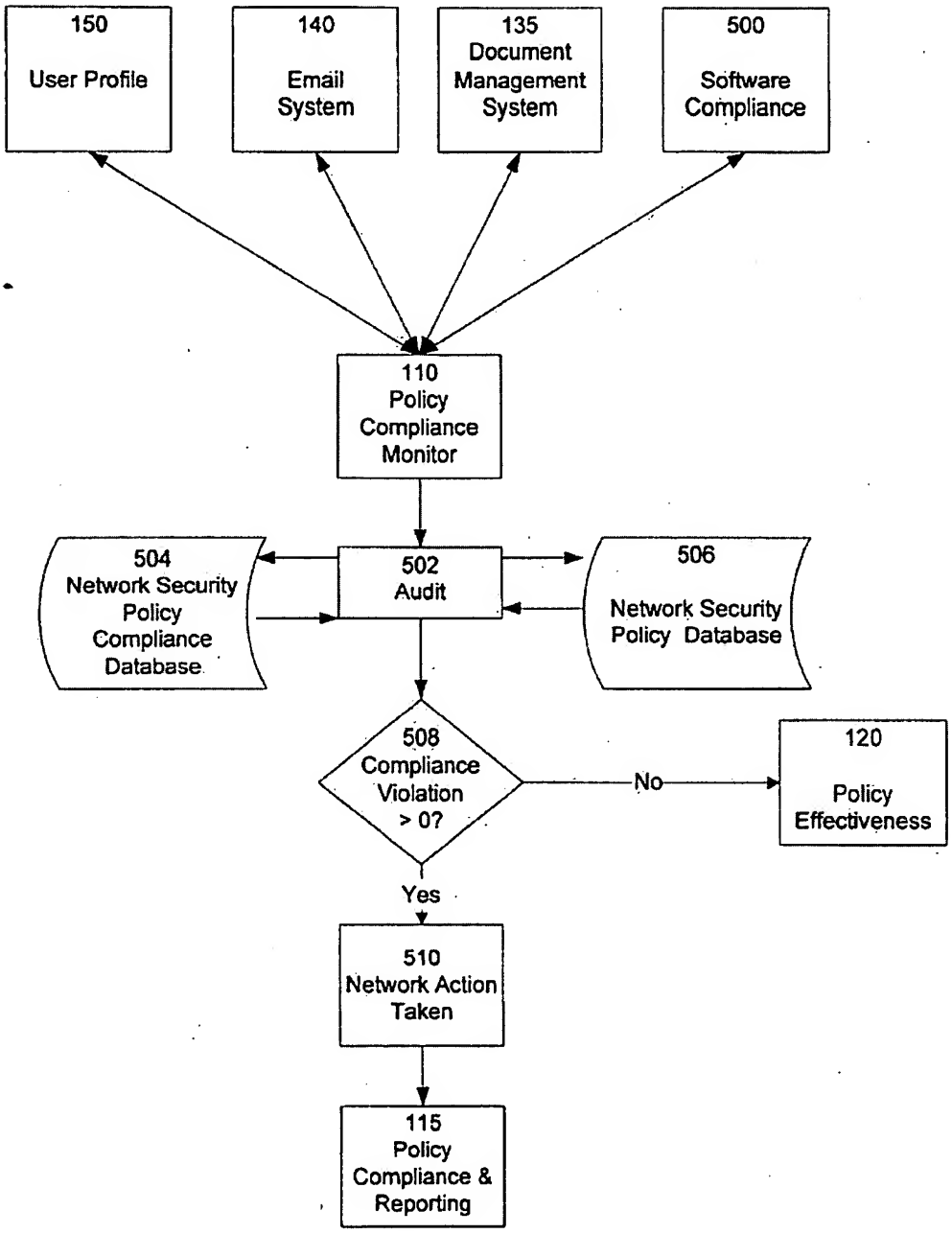


FIG. 6

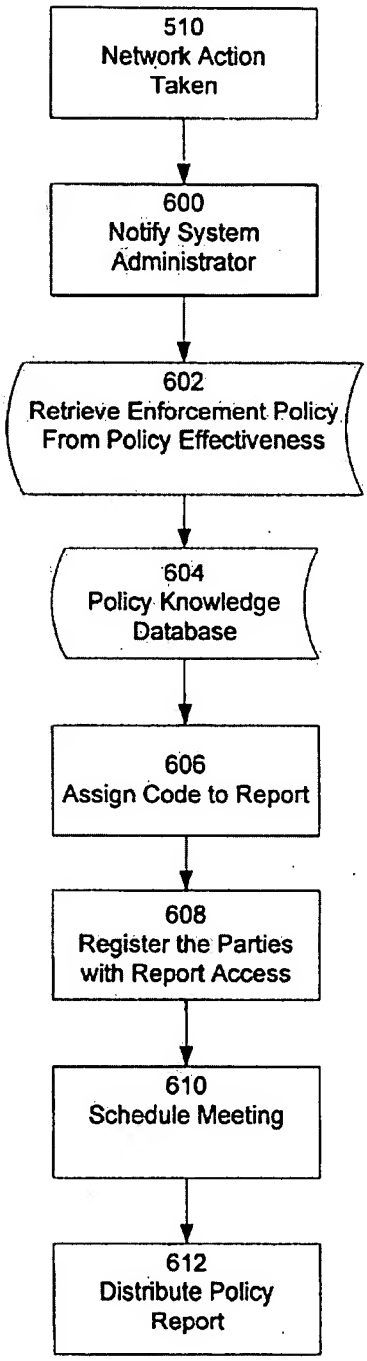


FIG. 7

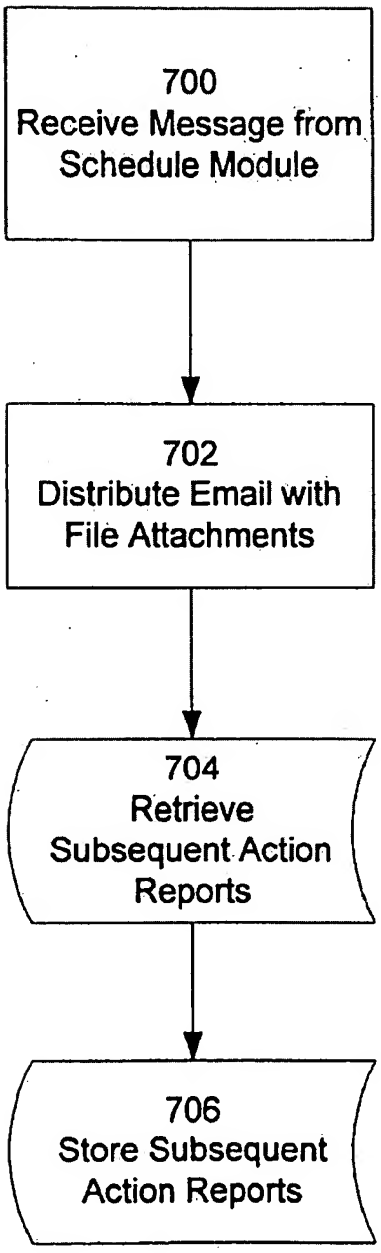


FIG. 8

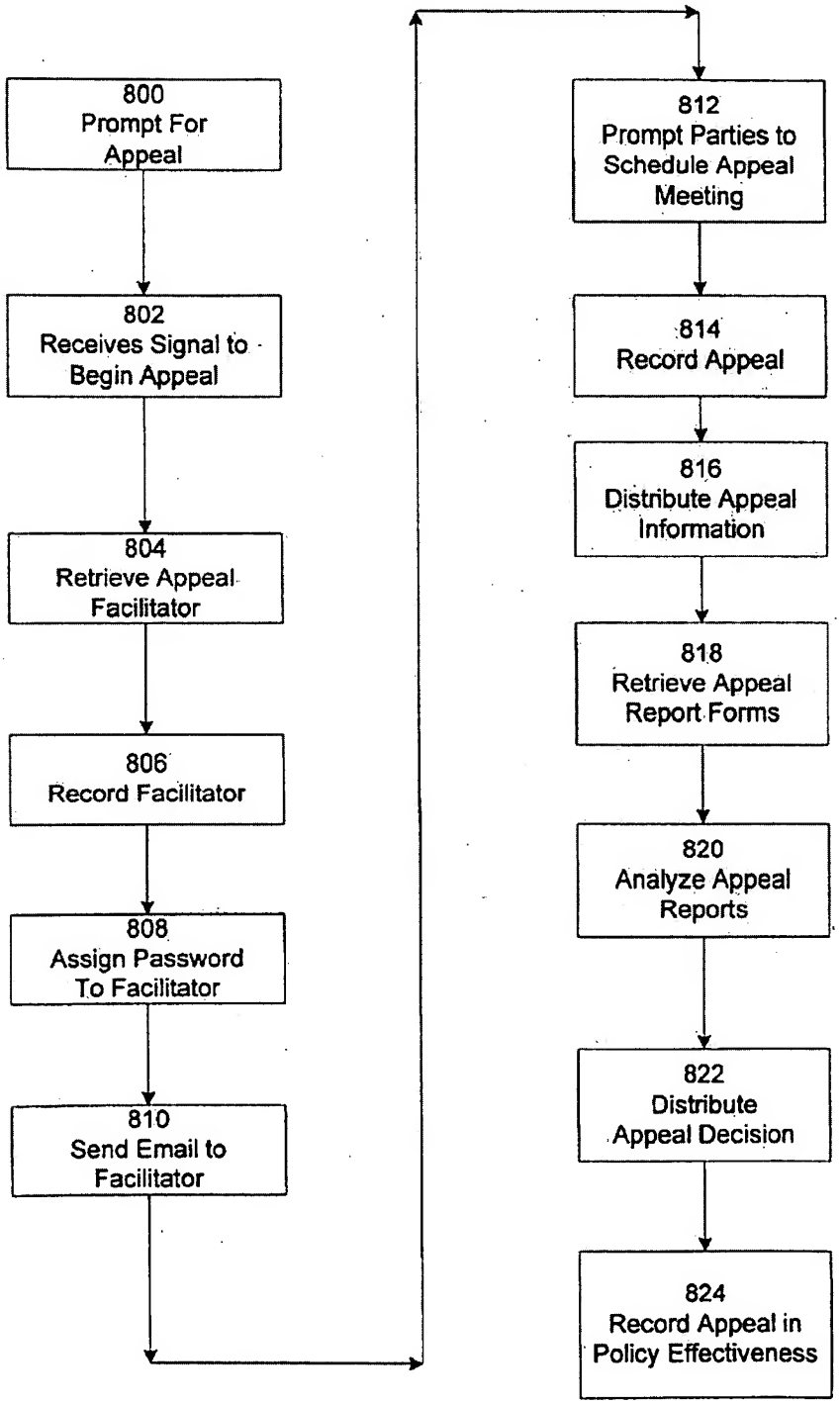


FIG. 9

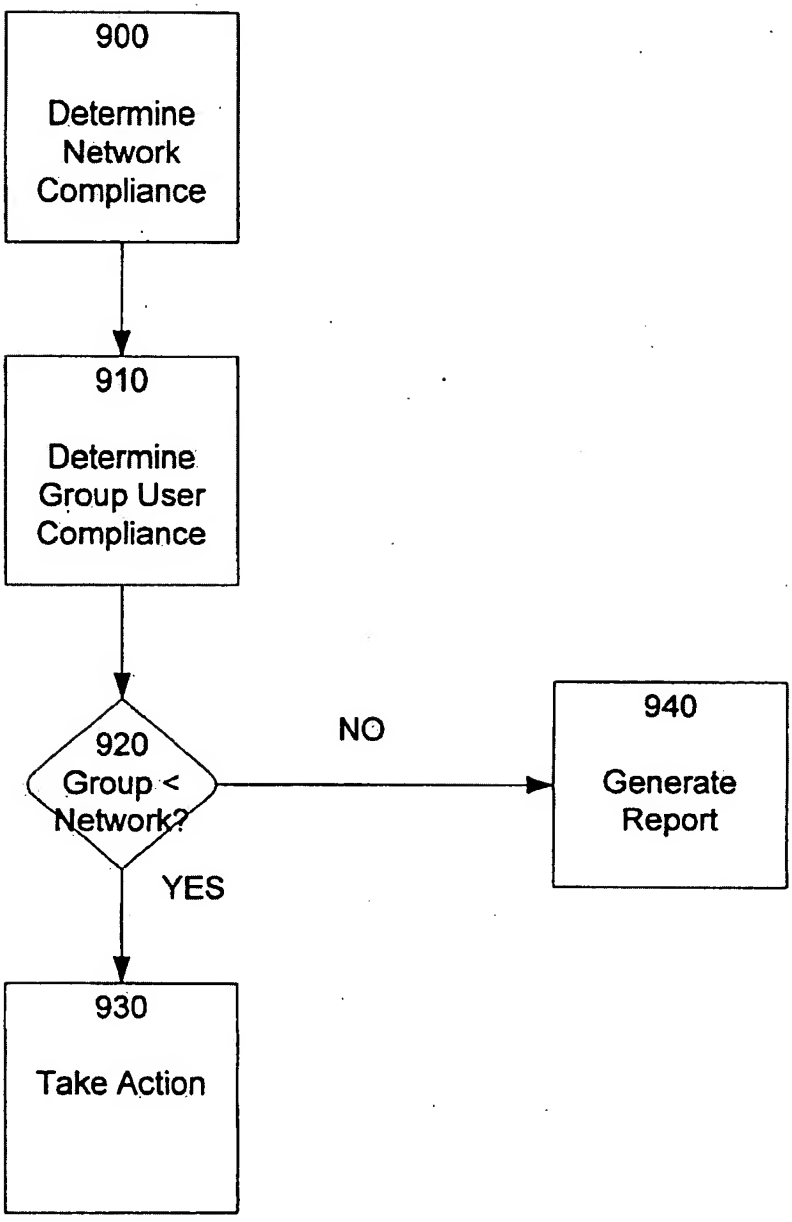


Figure 10

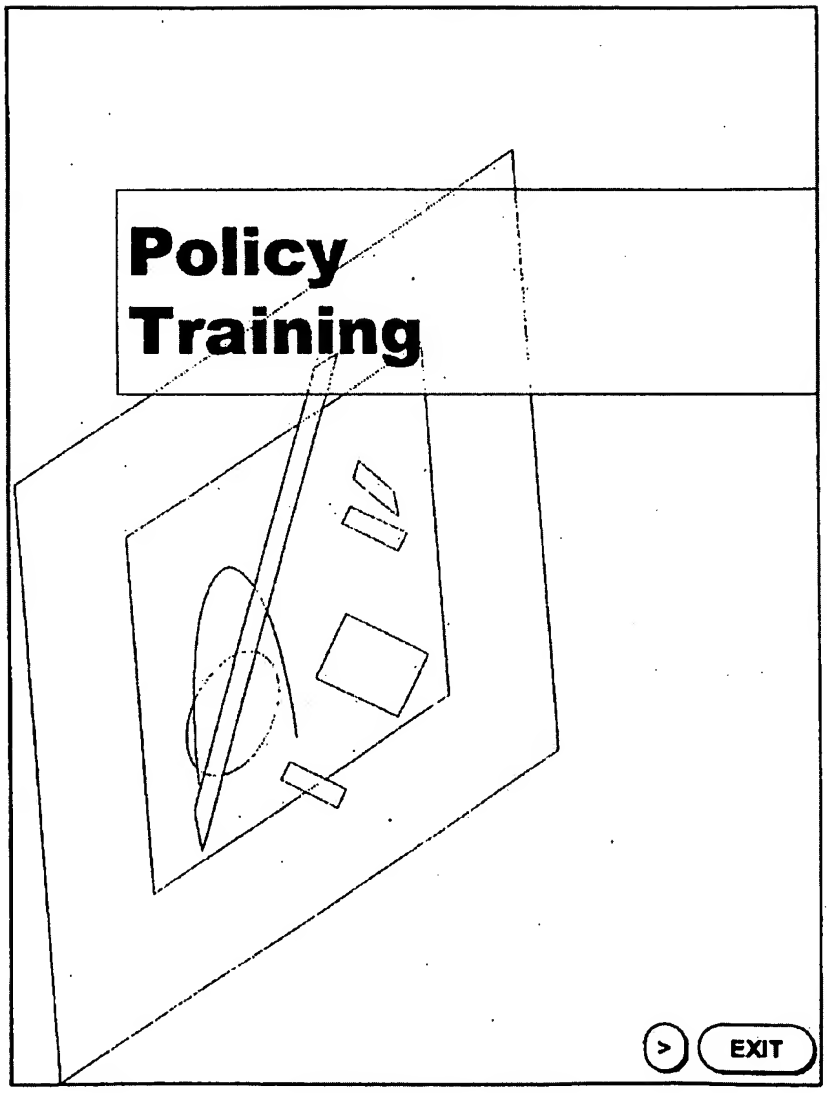


Figure 11

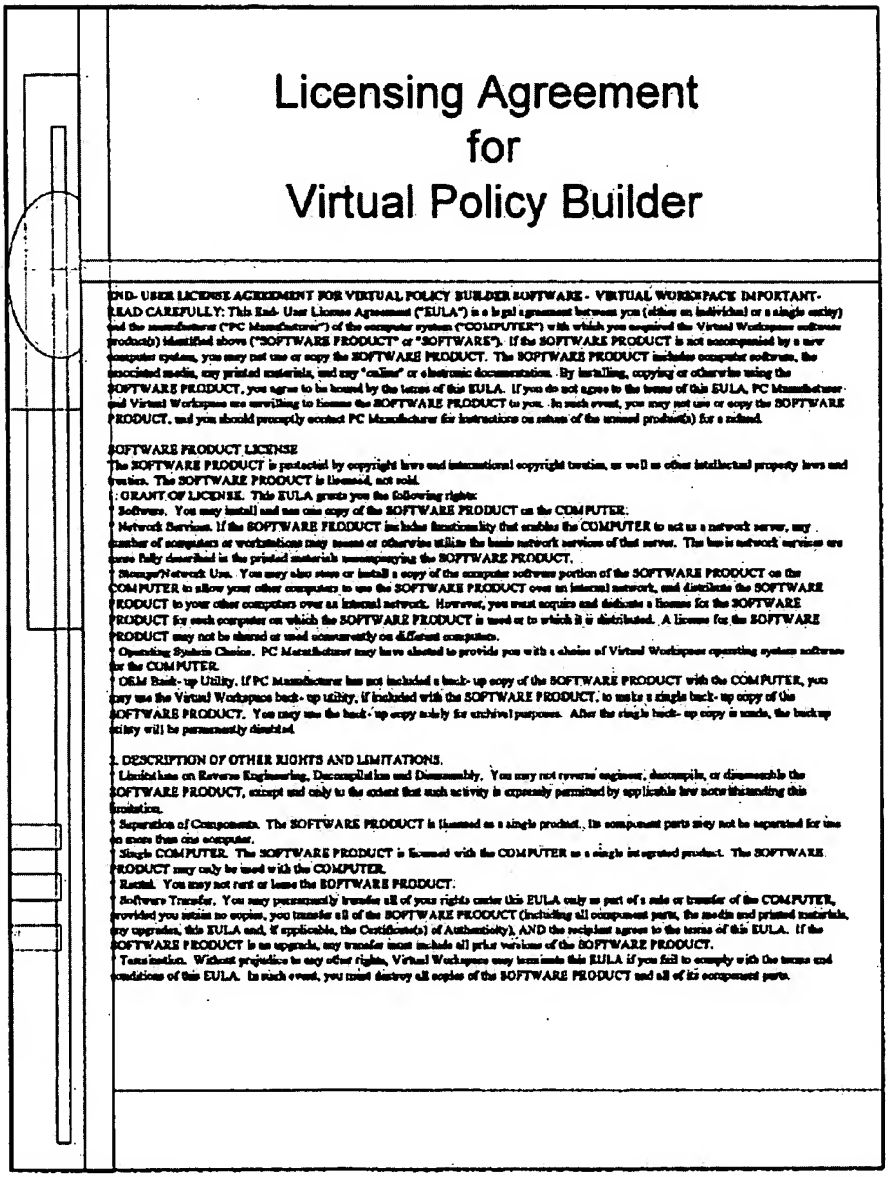


Figure 12

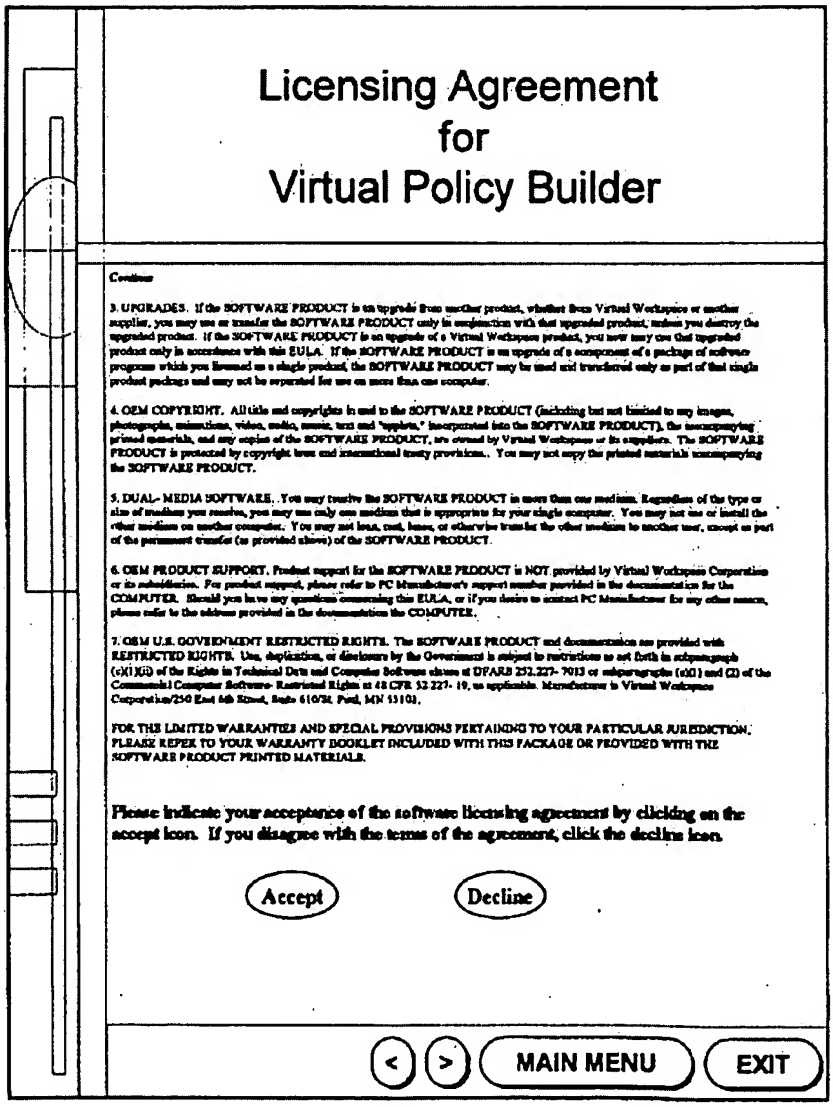


Figure 13

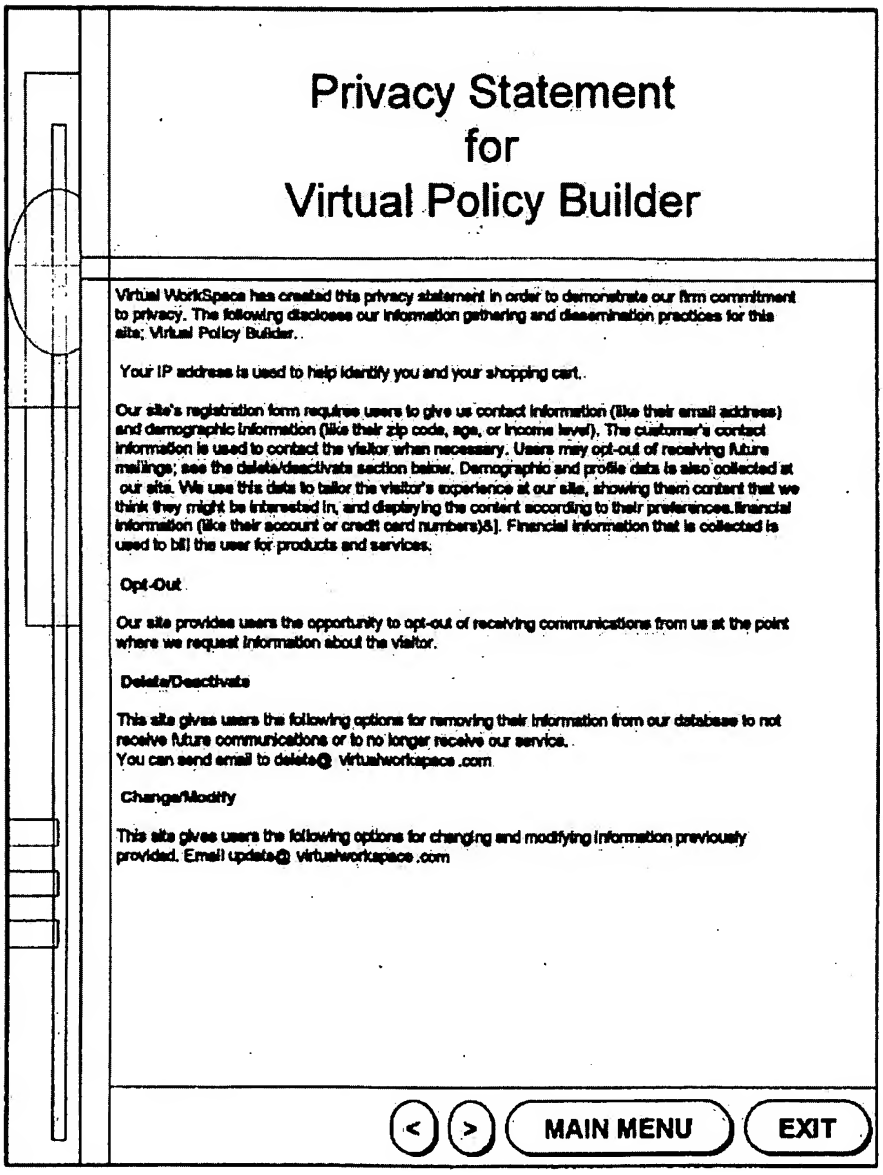

Privacy Statement
for
Virtual Policy Builder
Virtual WorkSpace has created this privacy statement in order to demonstrate our firm commitment to privacy. The following discloses our information gathering and dissemination practices for this site; Virtual Policy Builder.
Your IP address is used to help identify you and your shopping cart.
Our site's registration form requires users to give us contact information (like their email address) and demographic information (like their zip code, age, or income level). The customer's contact information is used to contact the visitor when necessary. Users may opt-out of receiving future mailings; see the delete/deactivate section below. Demographic and profile data is also collected at our site. We use this data to tailor the visitor's experience at our site, showing them content that we think they might be interested in, and displaying the content according to their preferences.finanicial information (like their account or credit card numbers)&]. Financial information that is collected is used to bill the user for products and services.
Opt-Out
Our site provides users the opportunity to opt-out of receiving communications from us at the point where we request information about the visitor.
Delete/Deactivate
This site gives users the following options for removing their information from our database to not receive future communications or to no longer receive our service.
You can send email to delete@ virtualworkspace .com
Change/Modify
This site gives users the following options for changing and modifying information previously provided. Email update@ virtualworkspace .com
<
>
MAIN MENU
EXIT

Figure 14

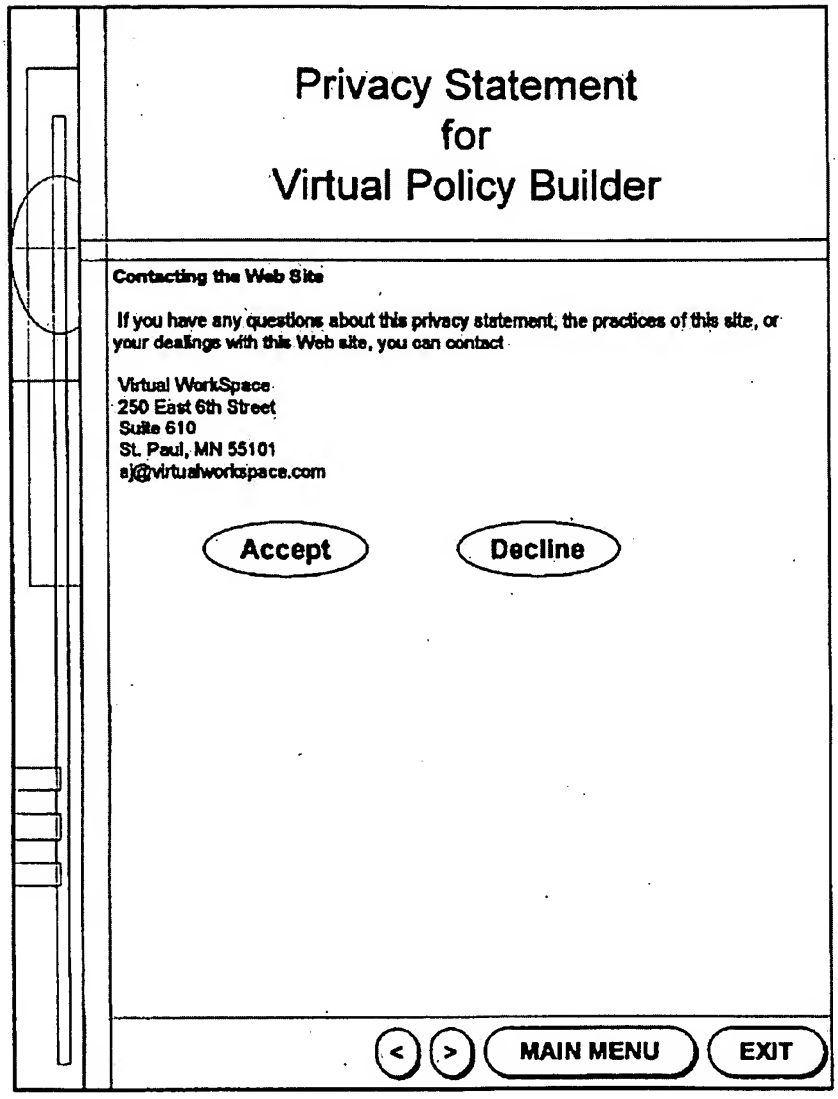


Figure 15

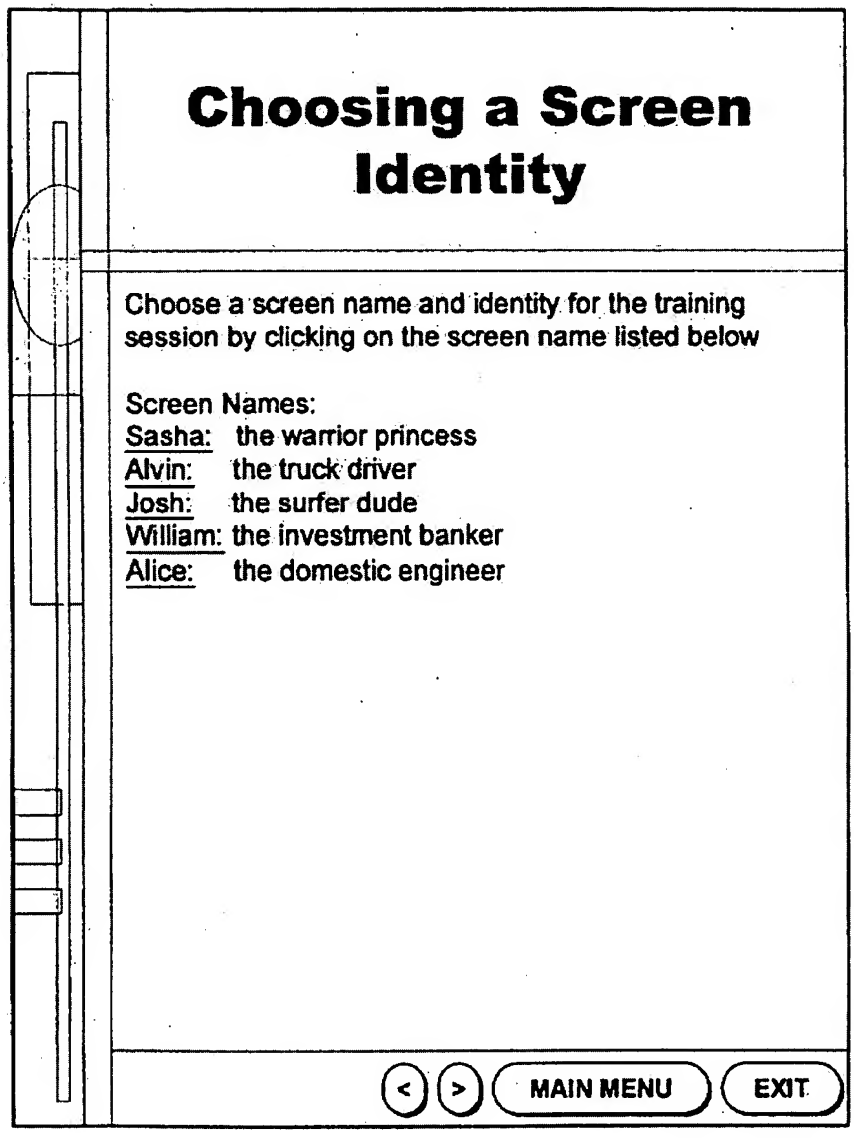


Figure 16

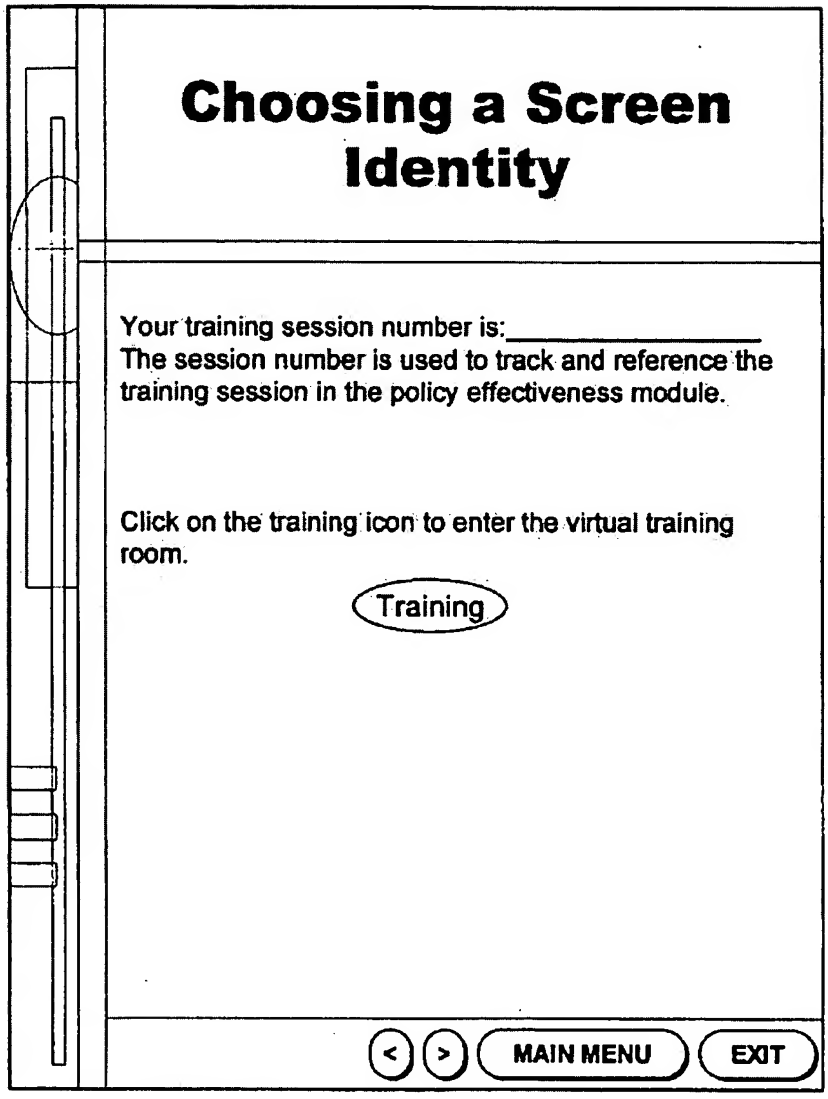


Figure 17

Figure 18

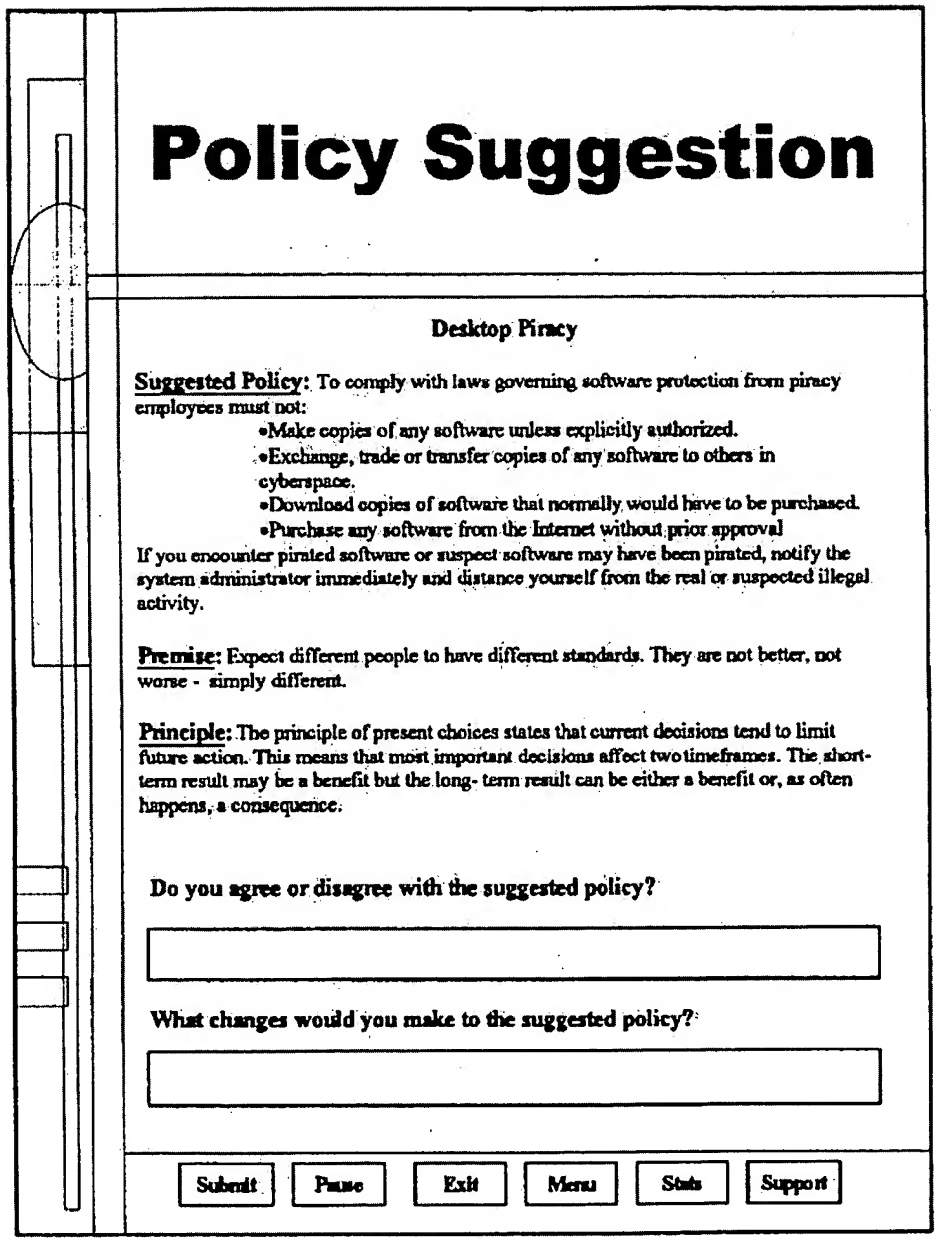


Figure 19

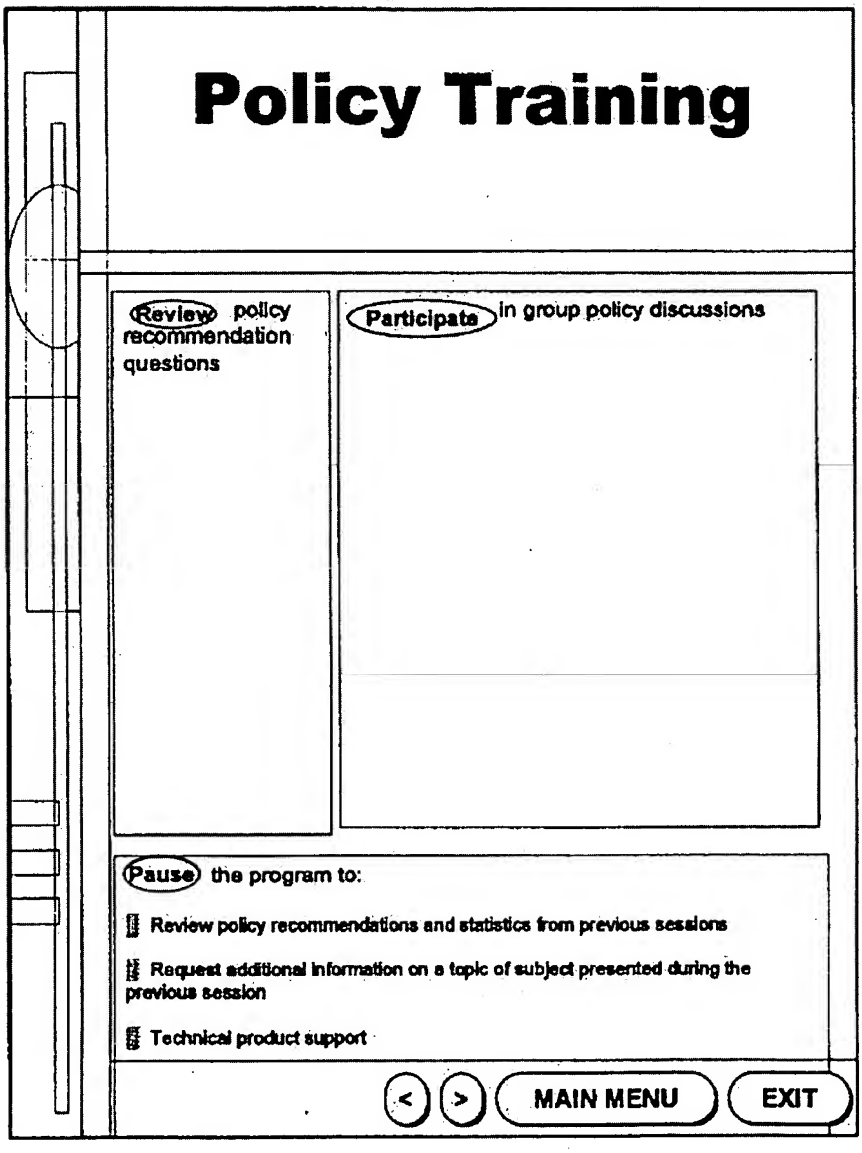


Figure 20

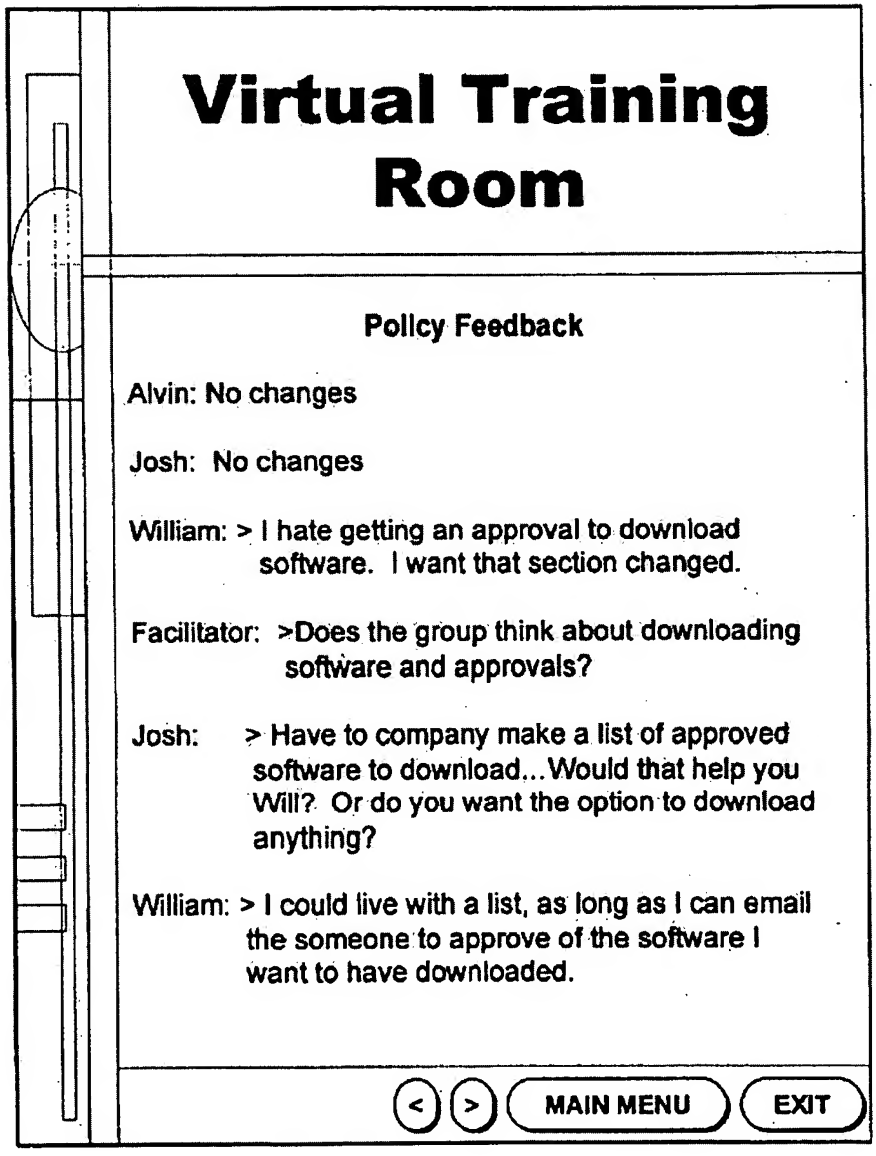


Figure 21

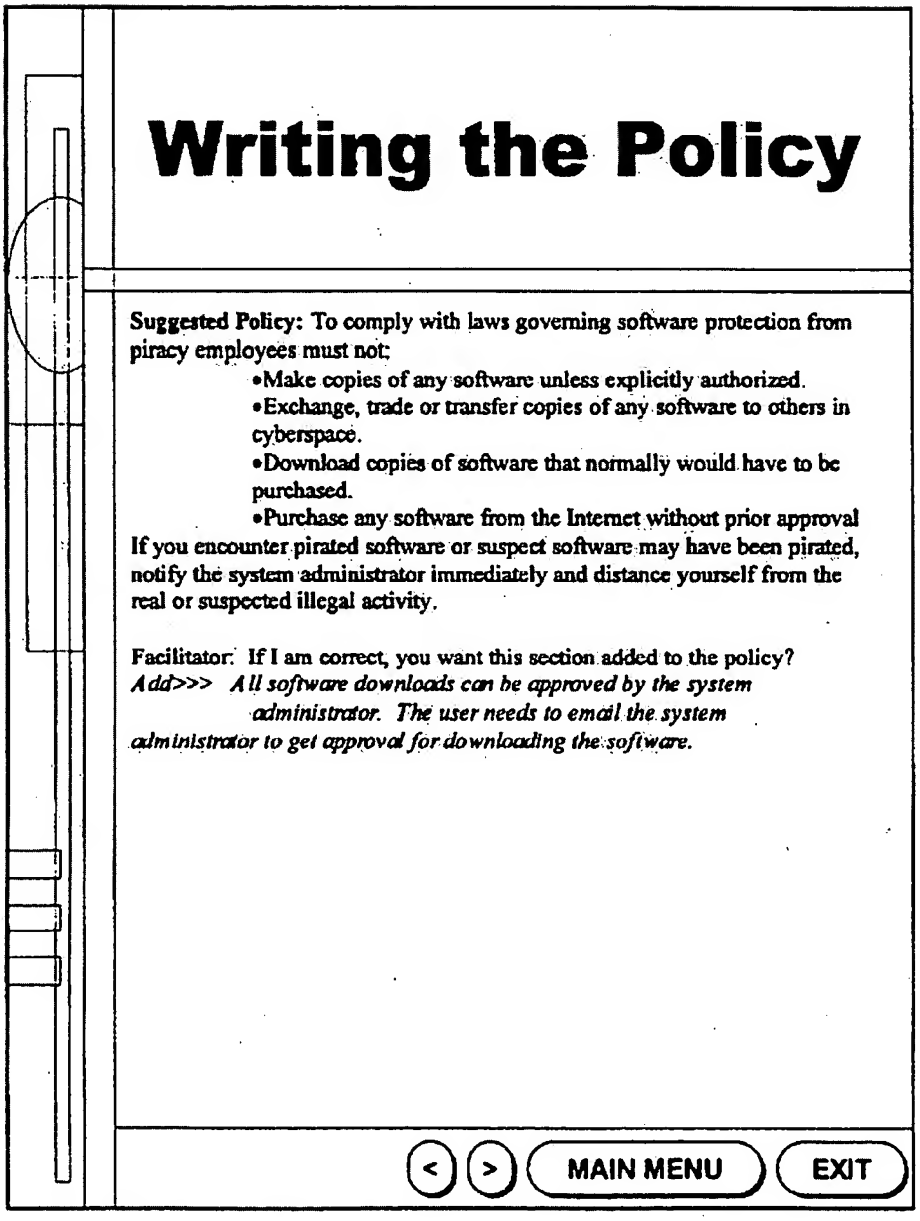


Figure 22

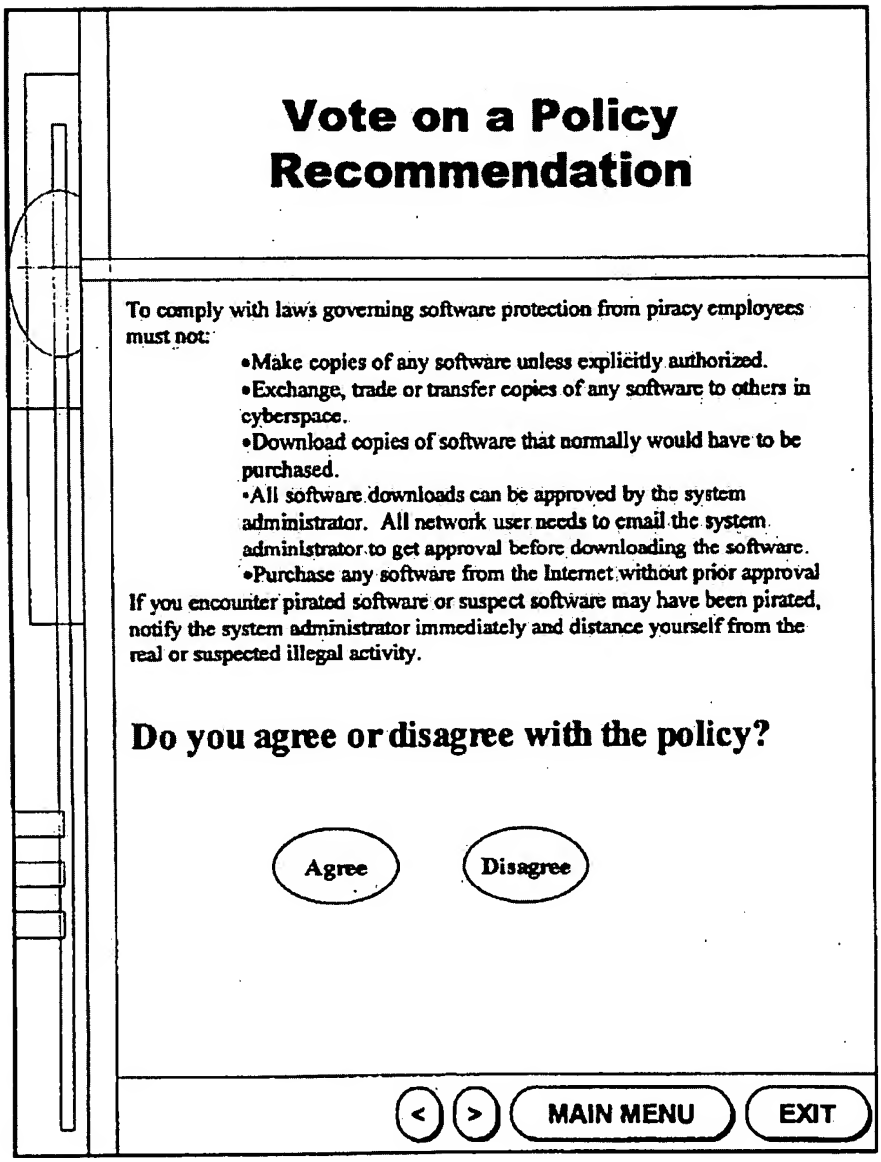


Figure 23

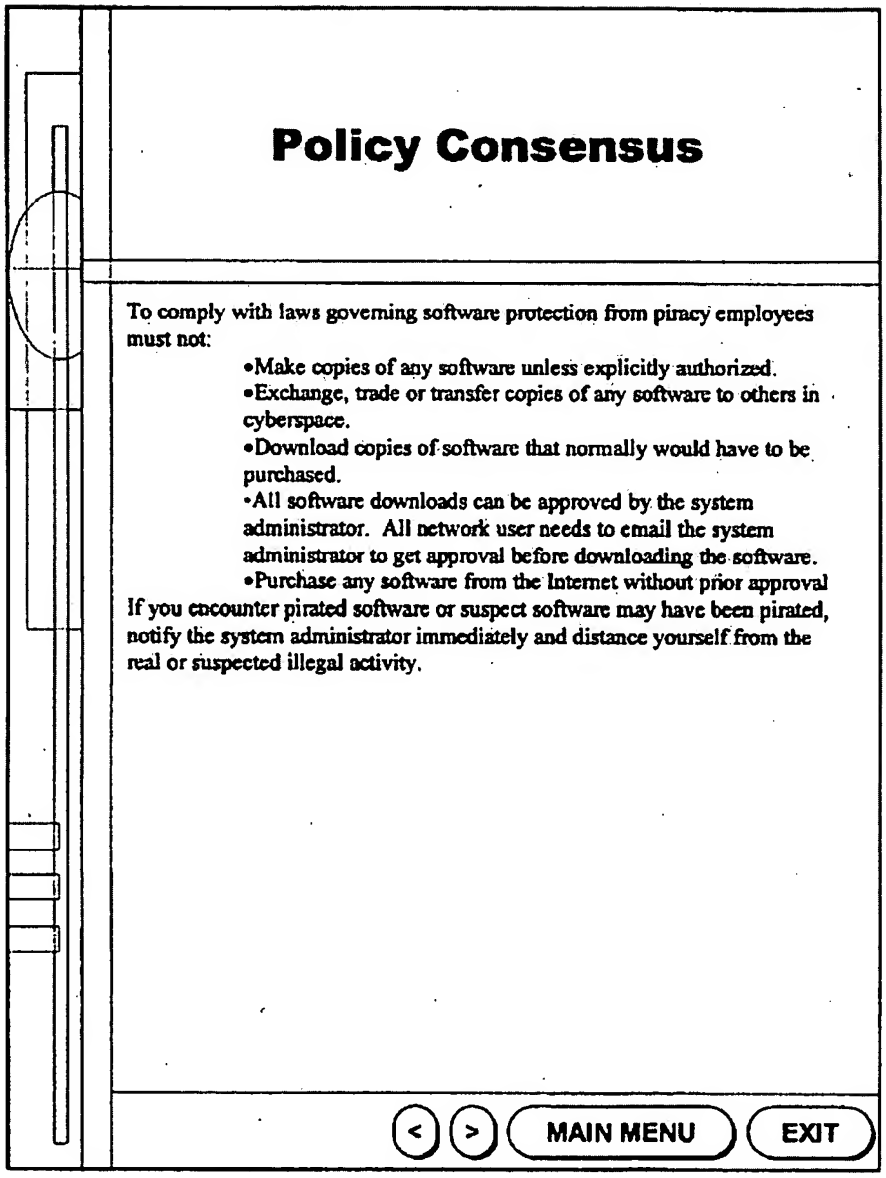


Figure 24

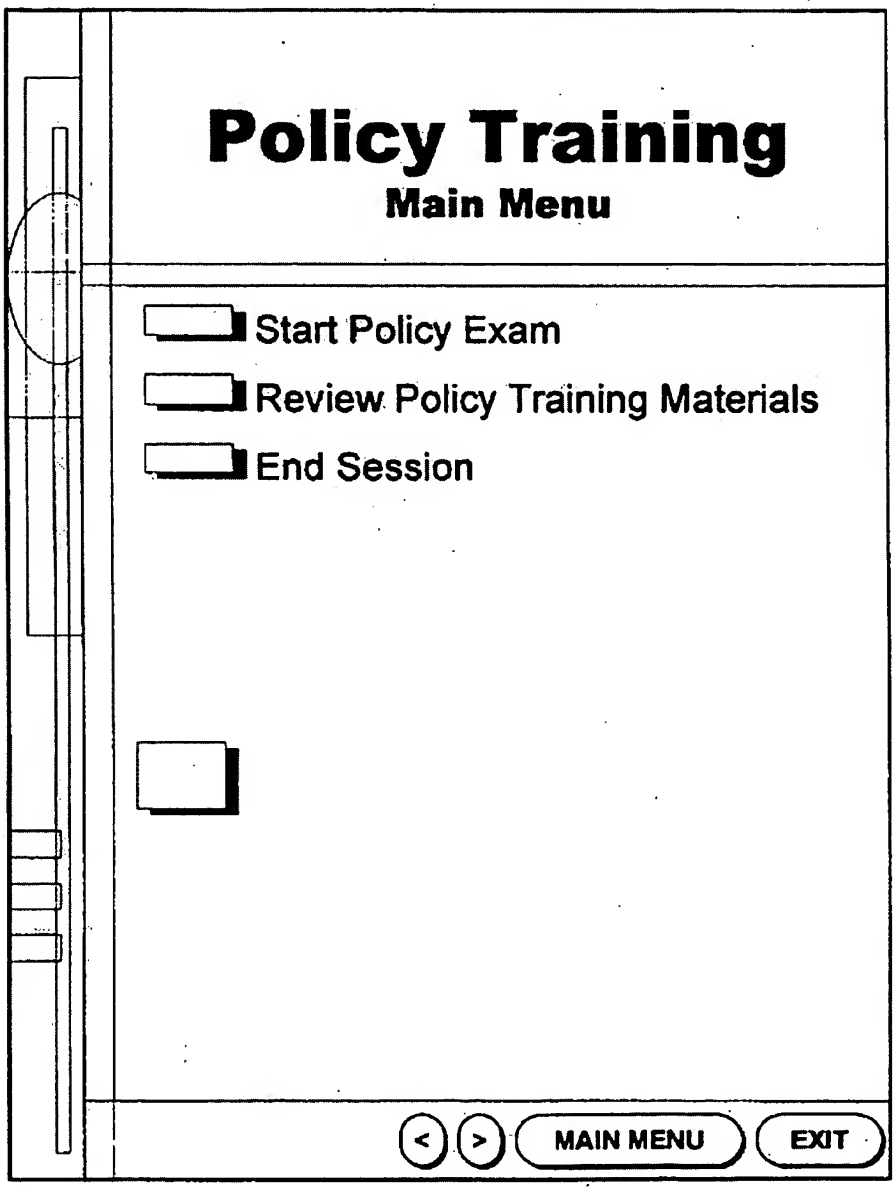


Figure 25

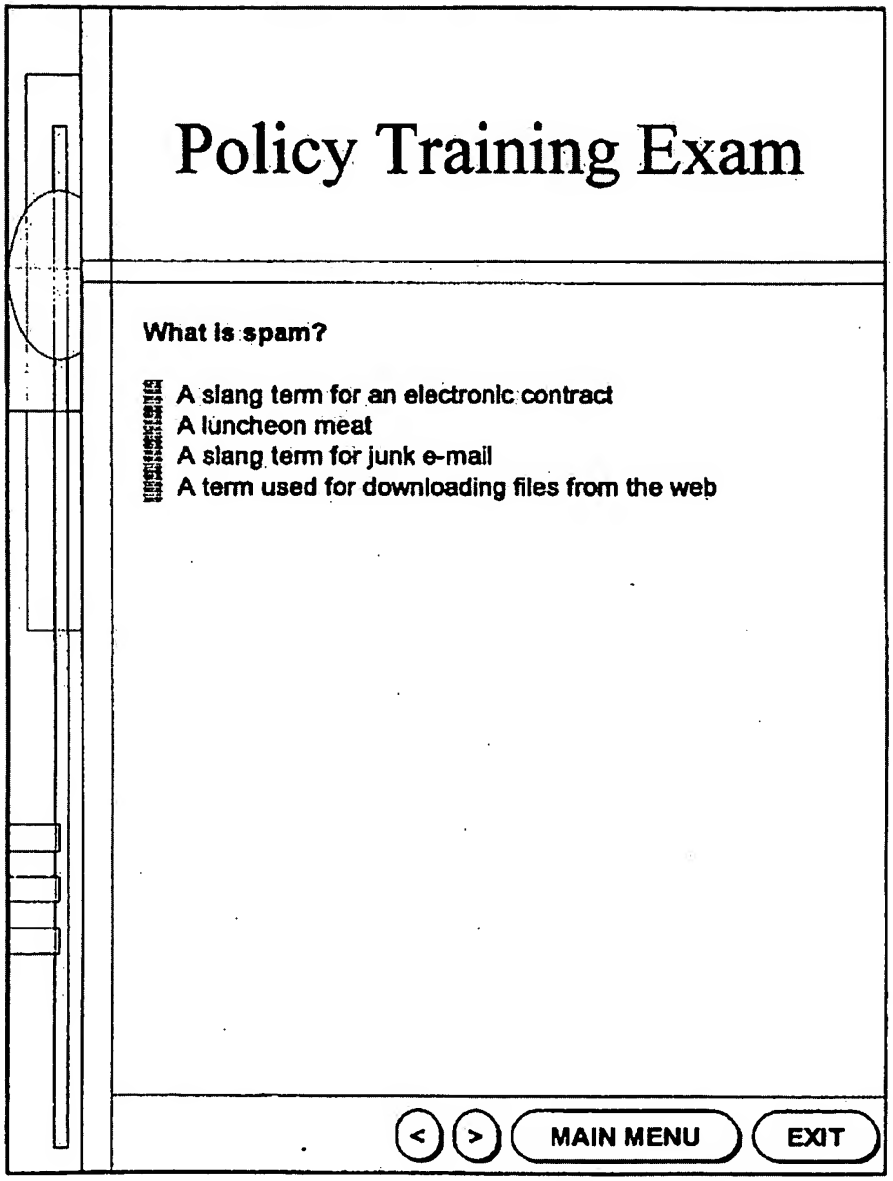


Figure 26

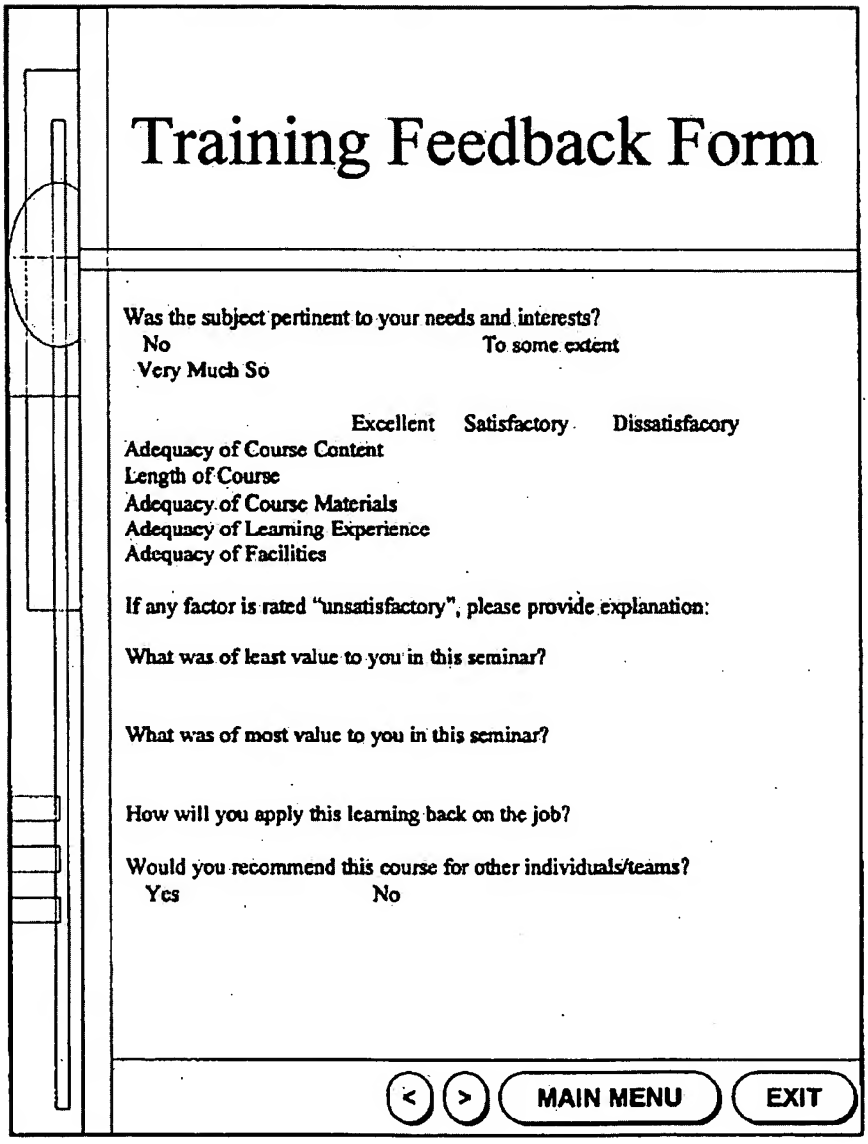


Figure 27

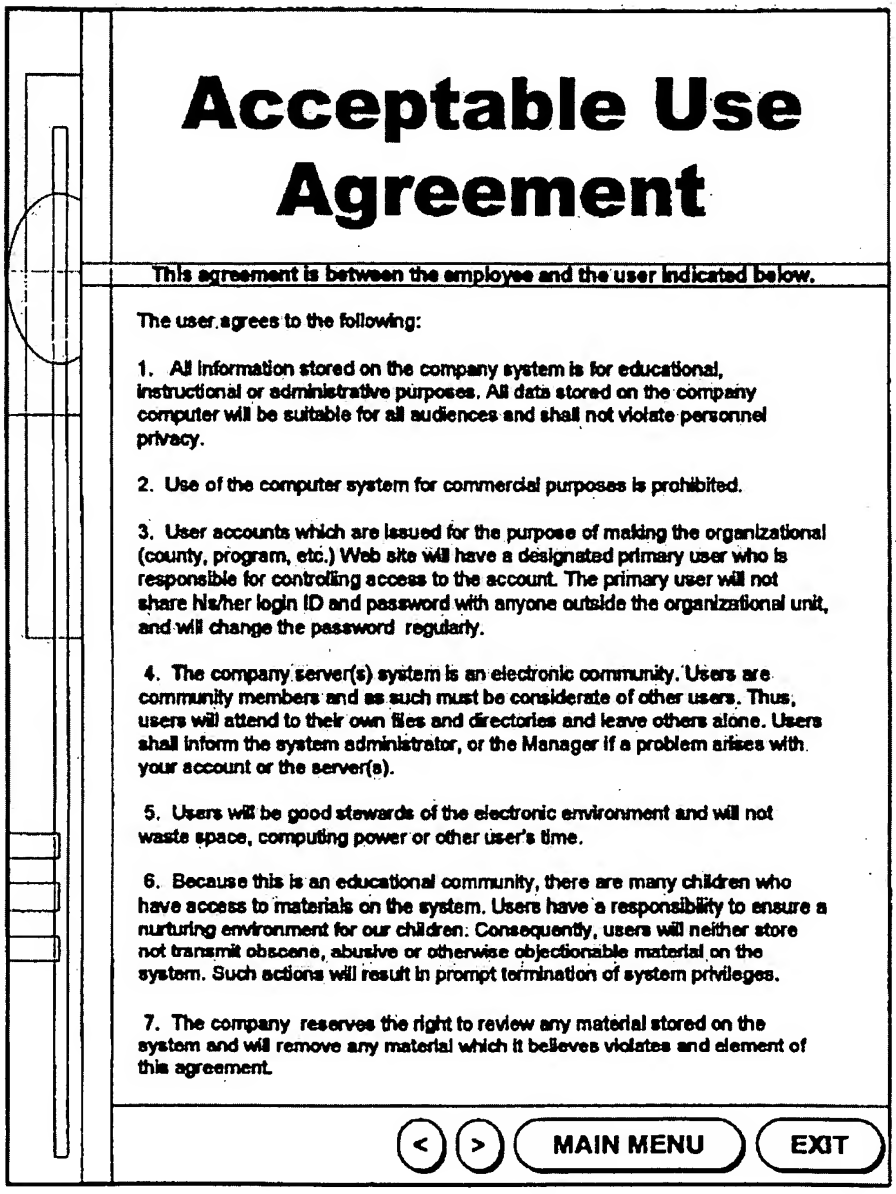


Figure 28

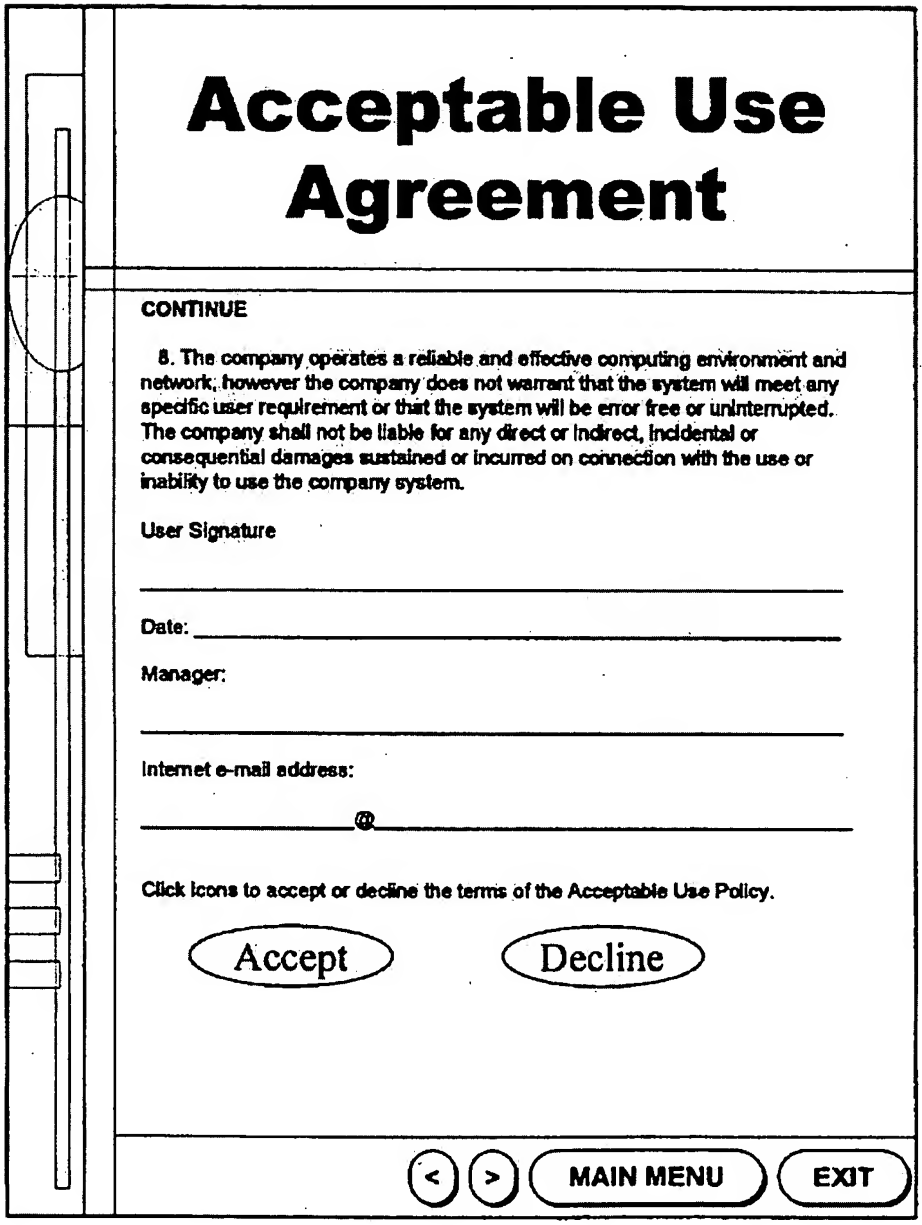


Figure 29

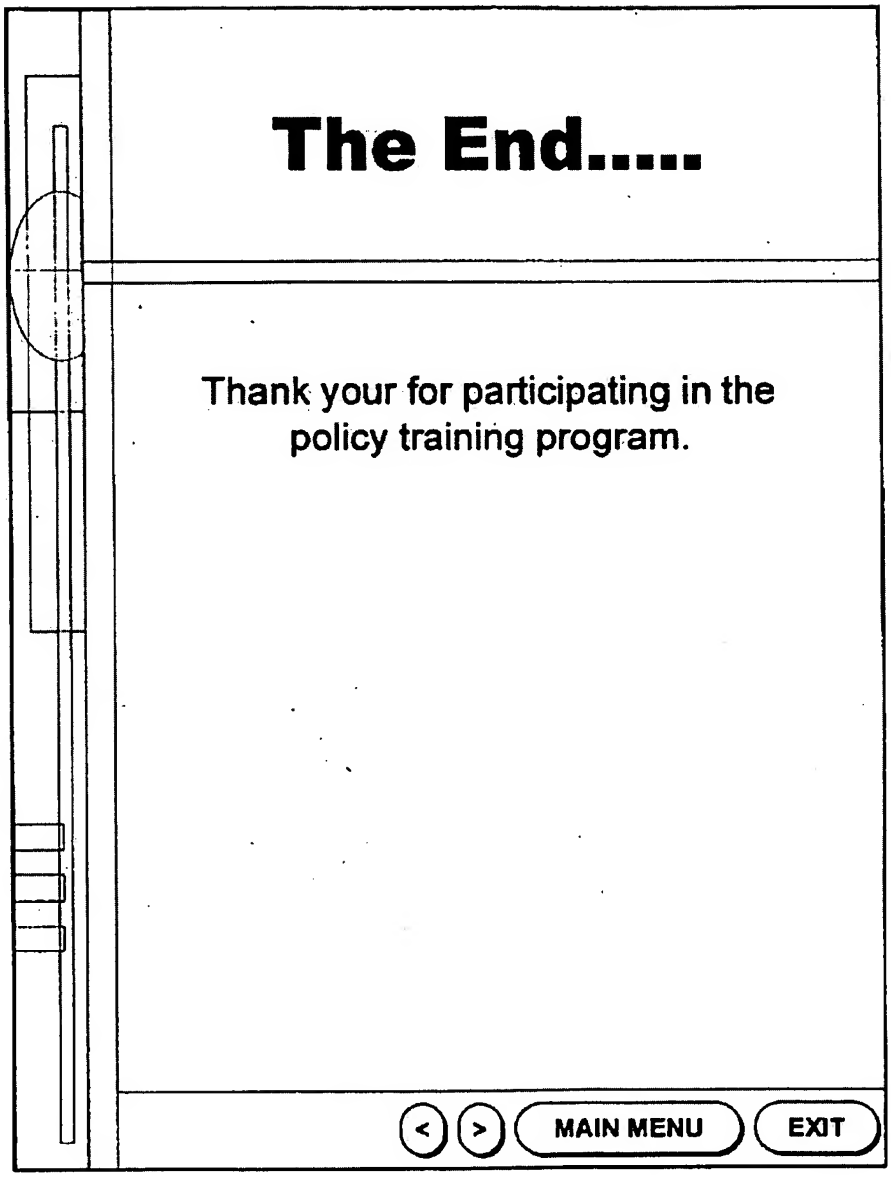


Figure 30

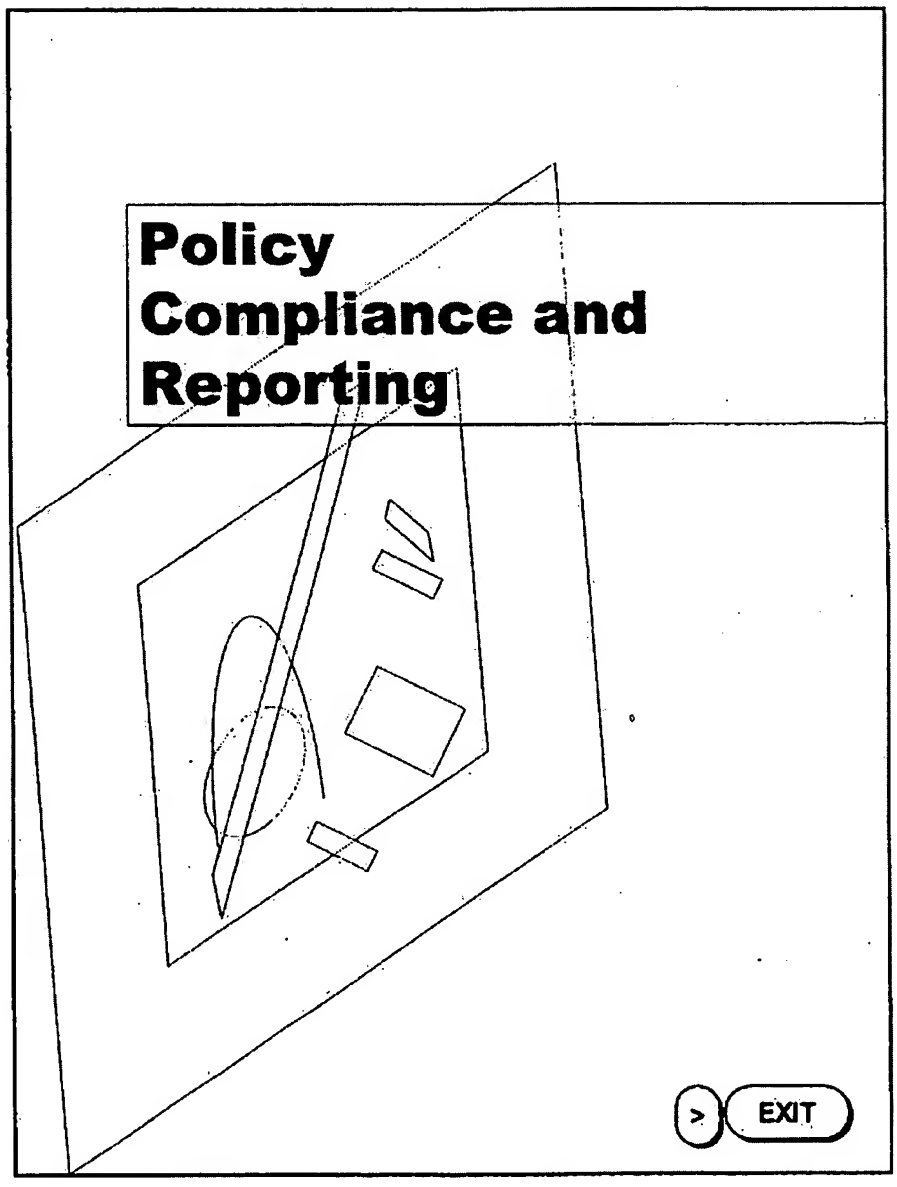


Figure 31

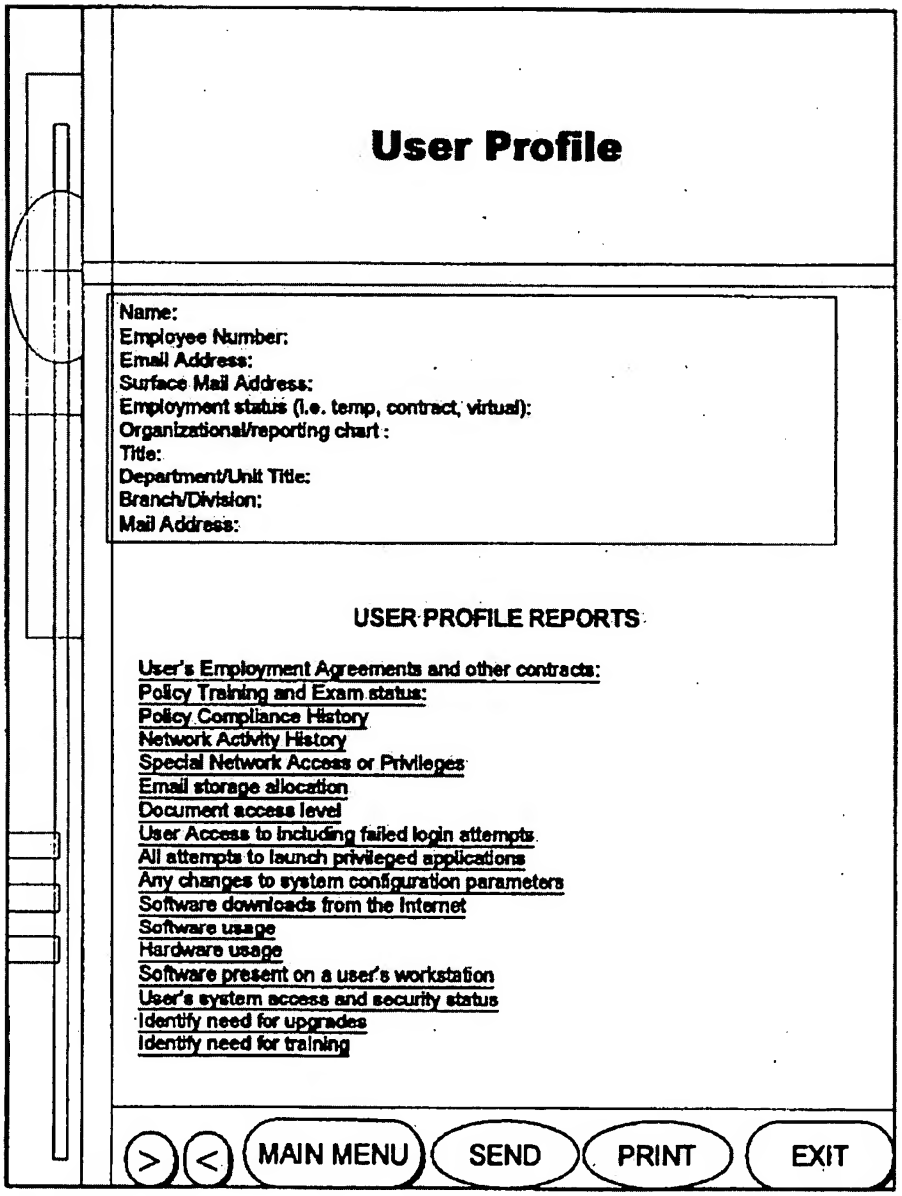


Figure 32

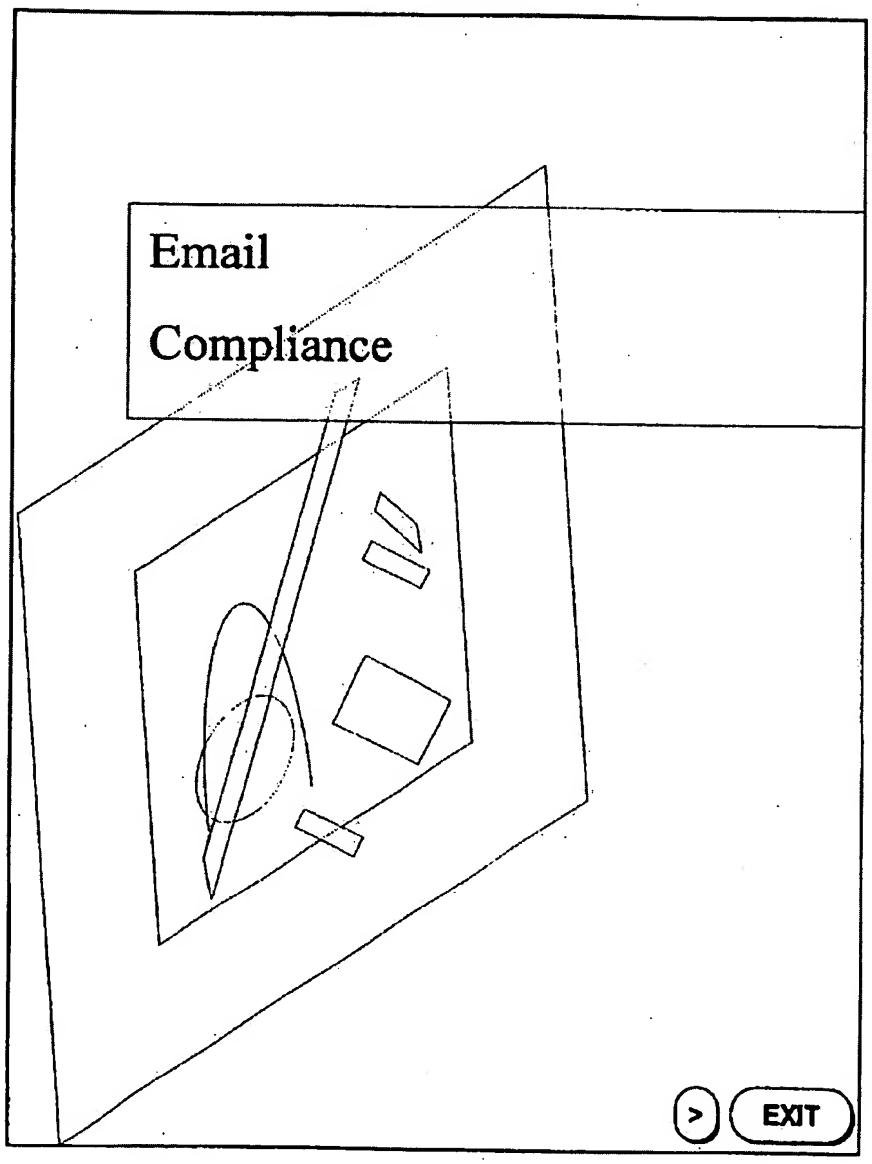


Figure 33

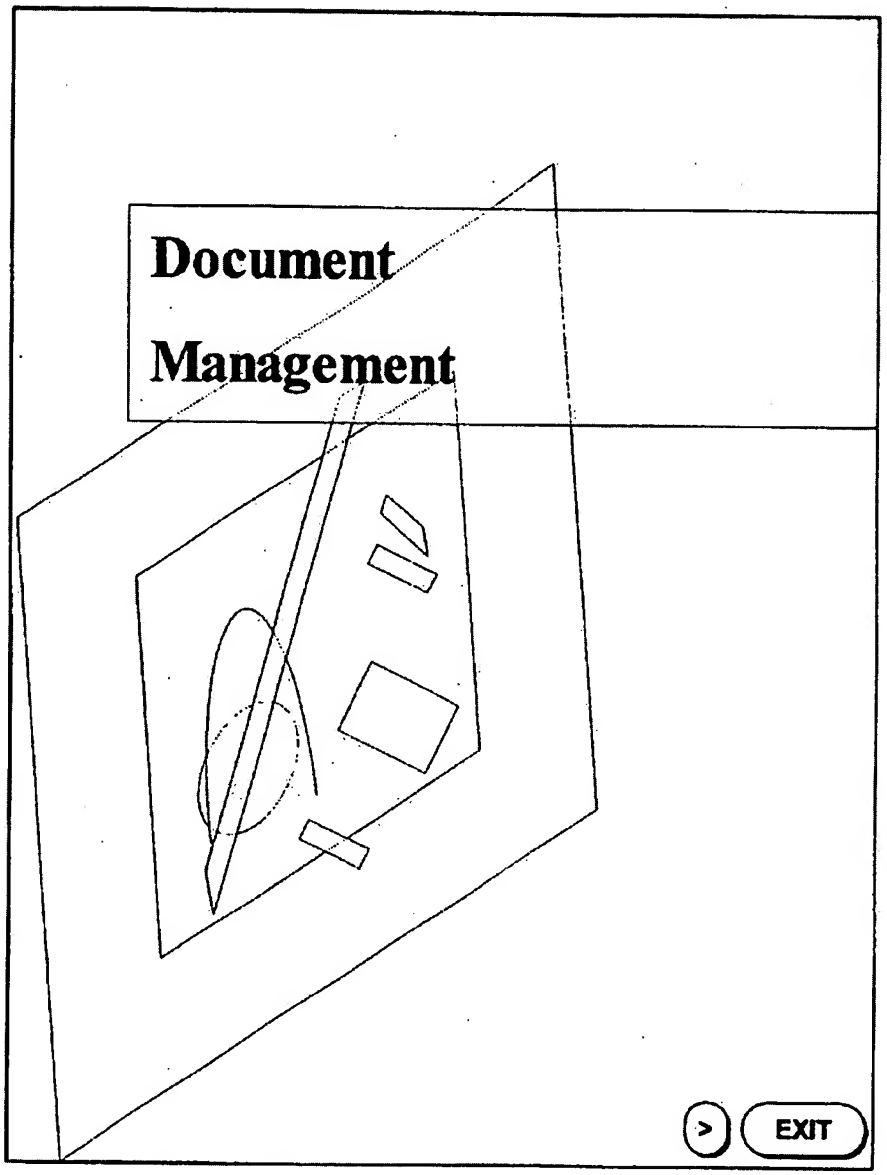


Figure 34

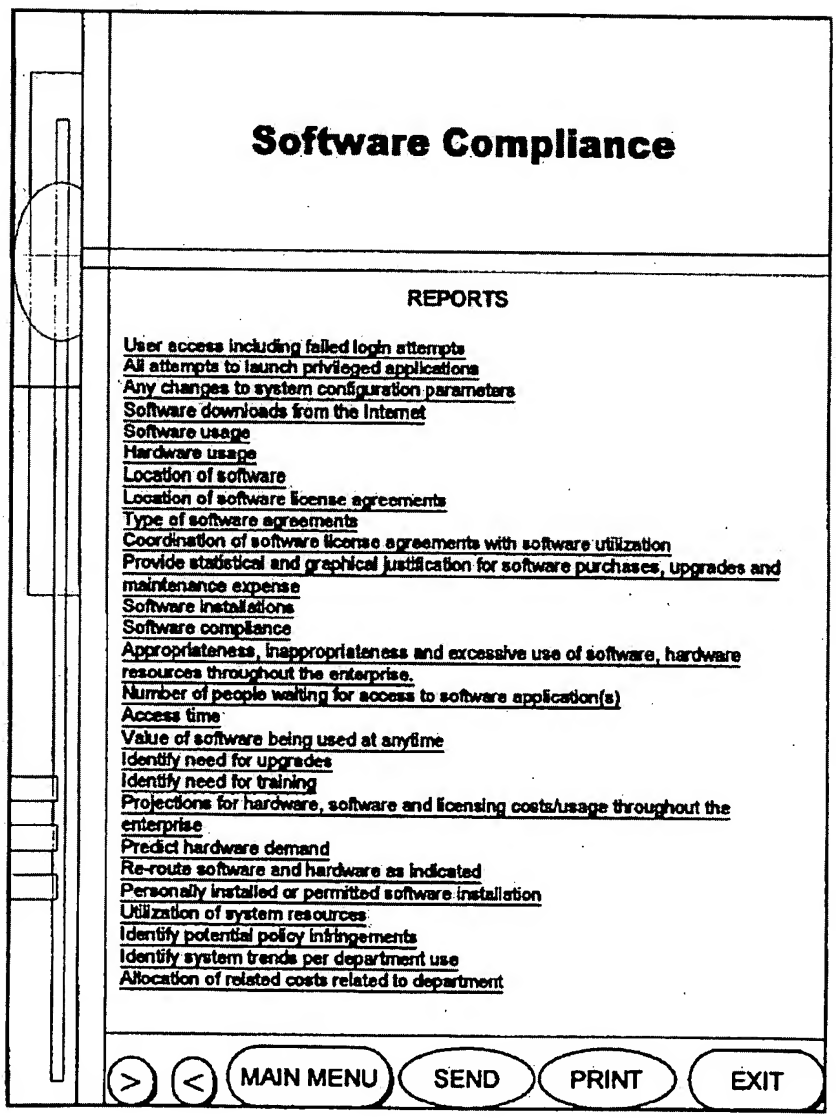


Figure 35

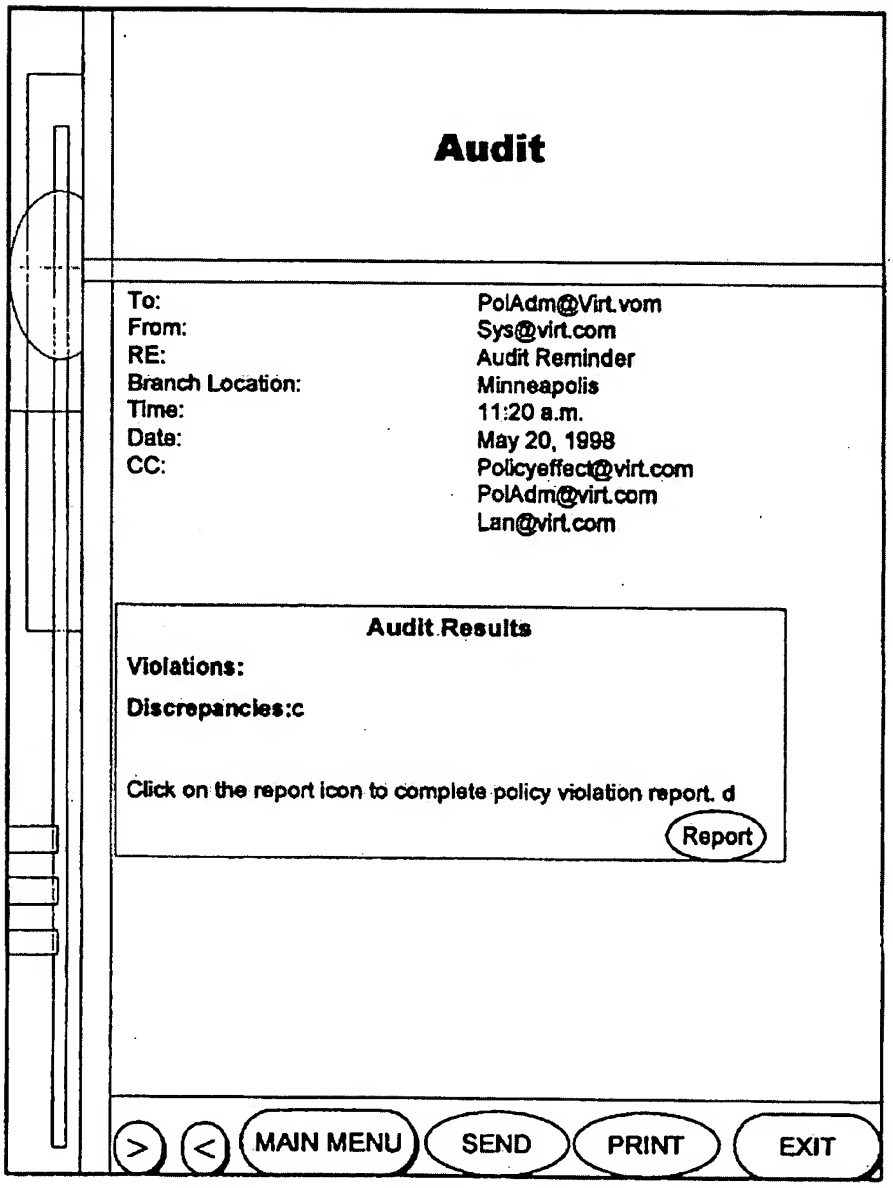


Figure 36

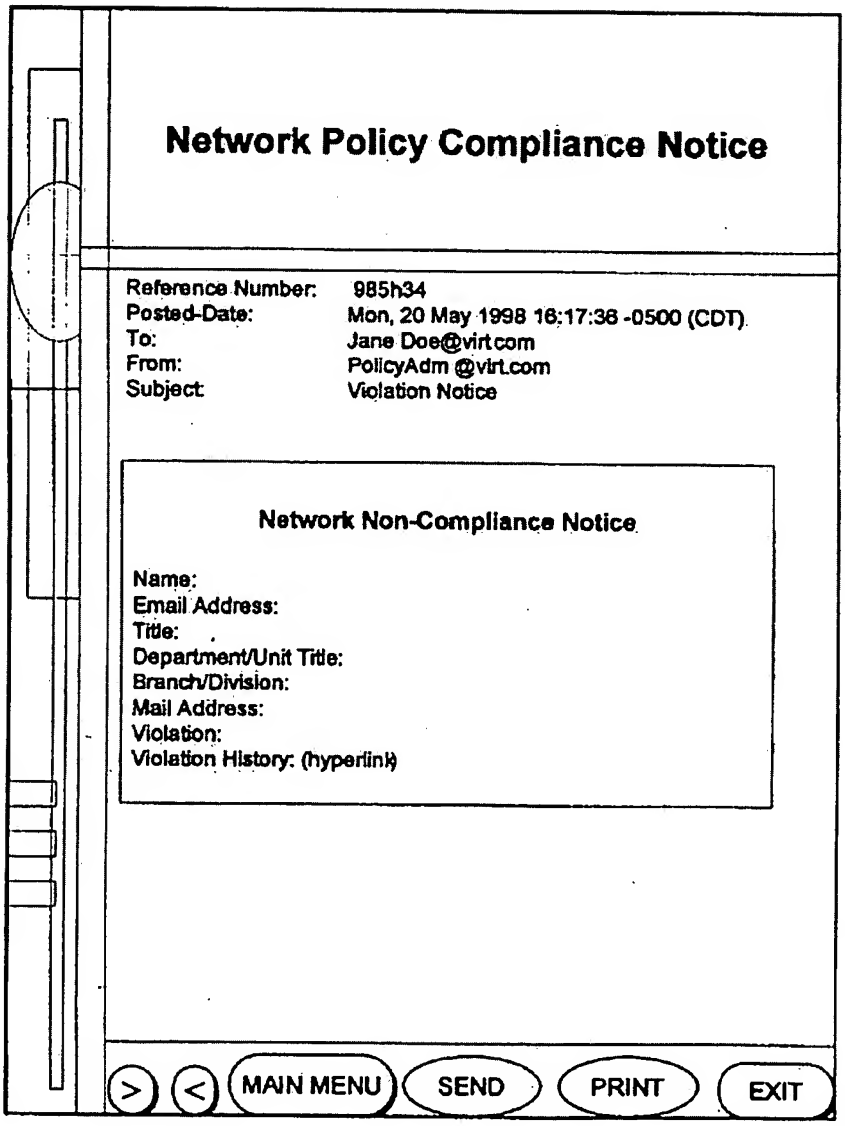


Figure 37

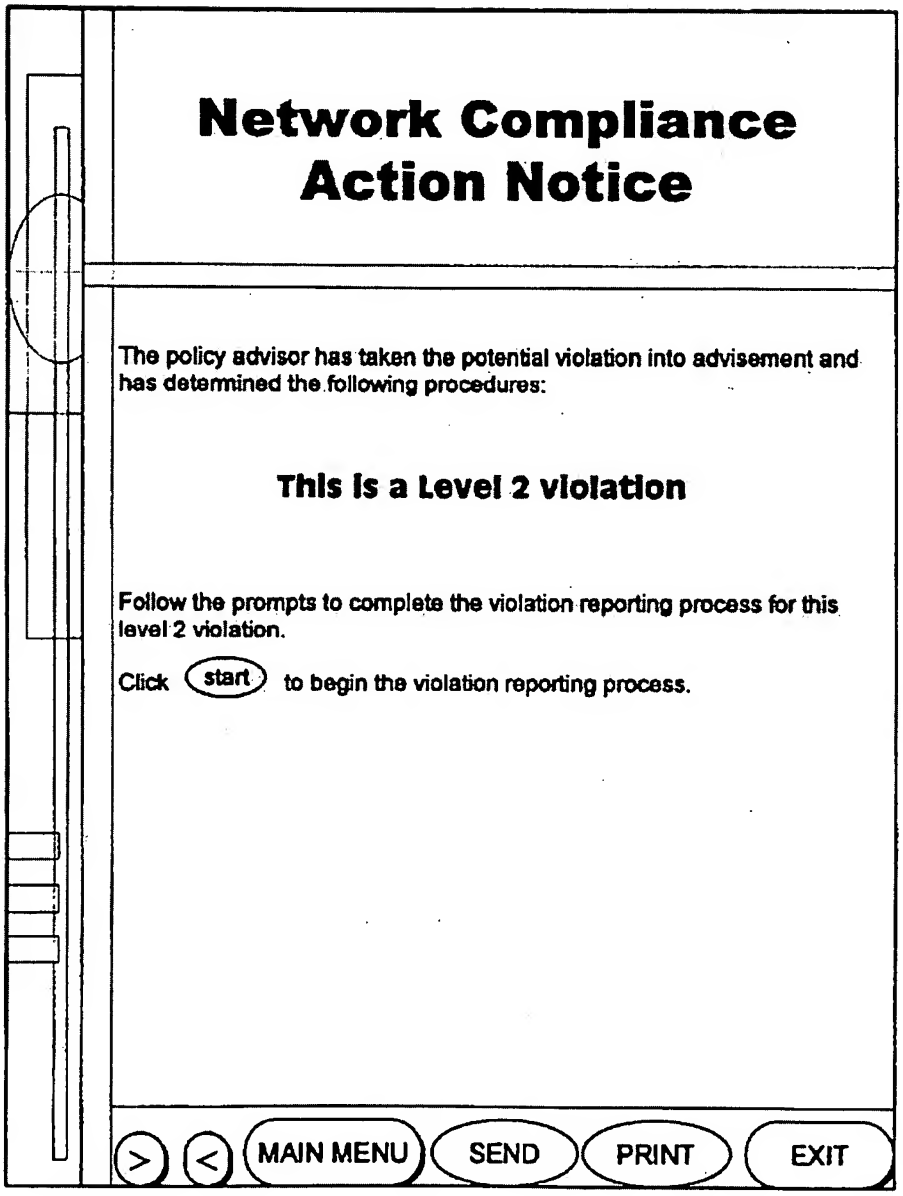


Figure 38

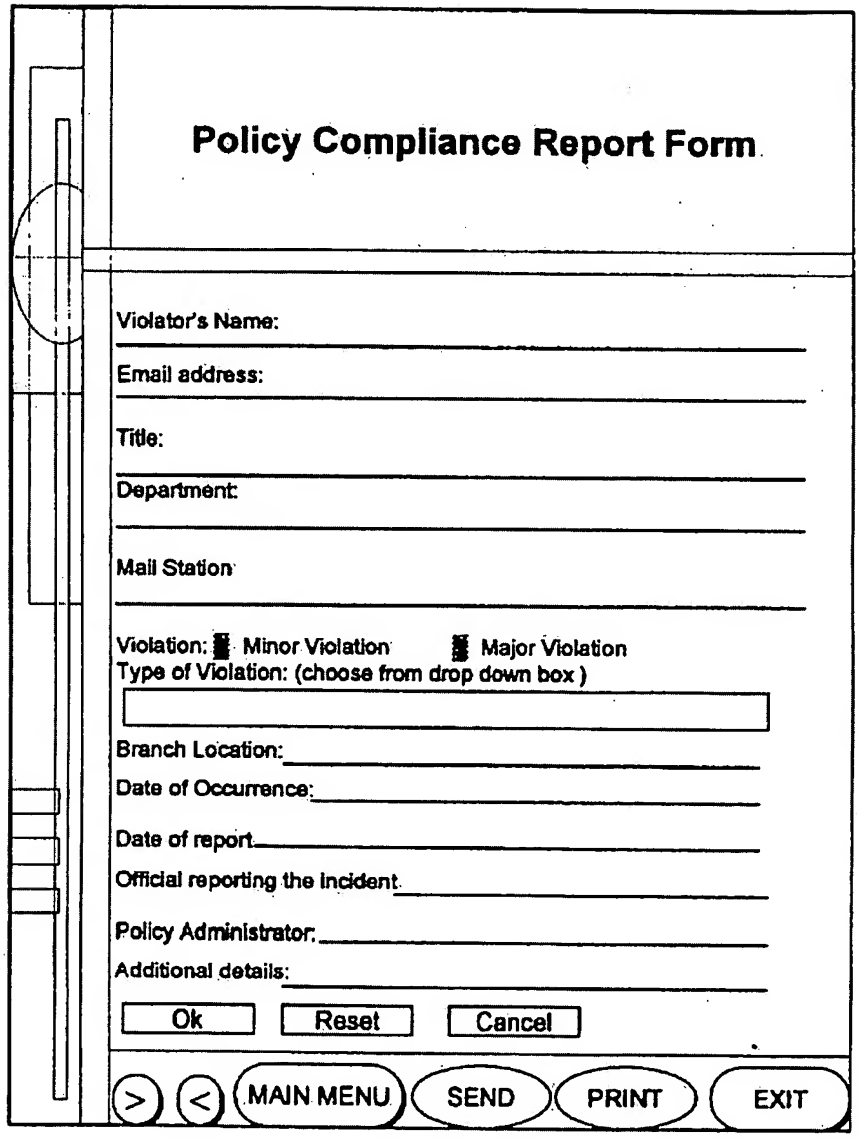


Figure 39

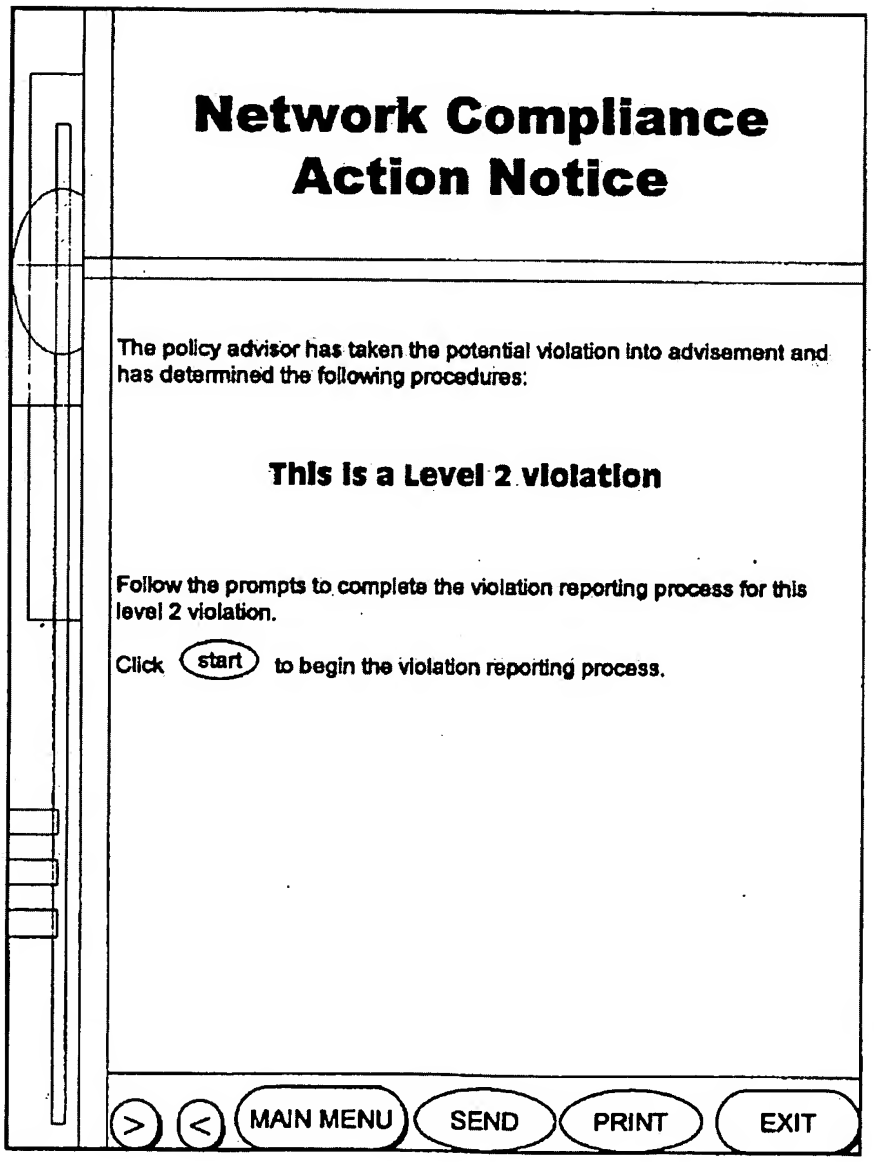


Figure 40

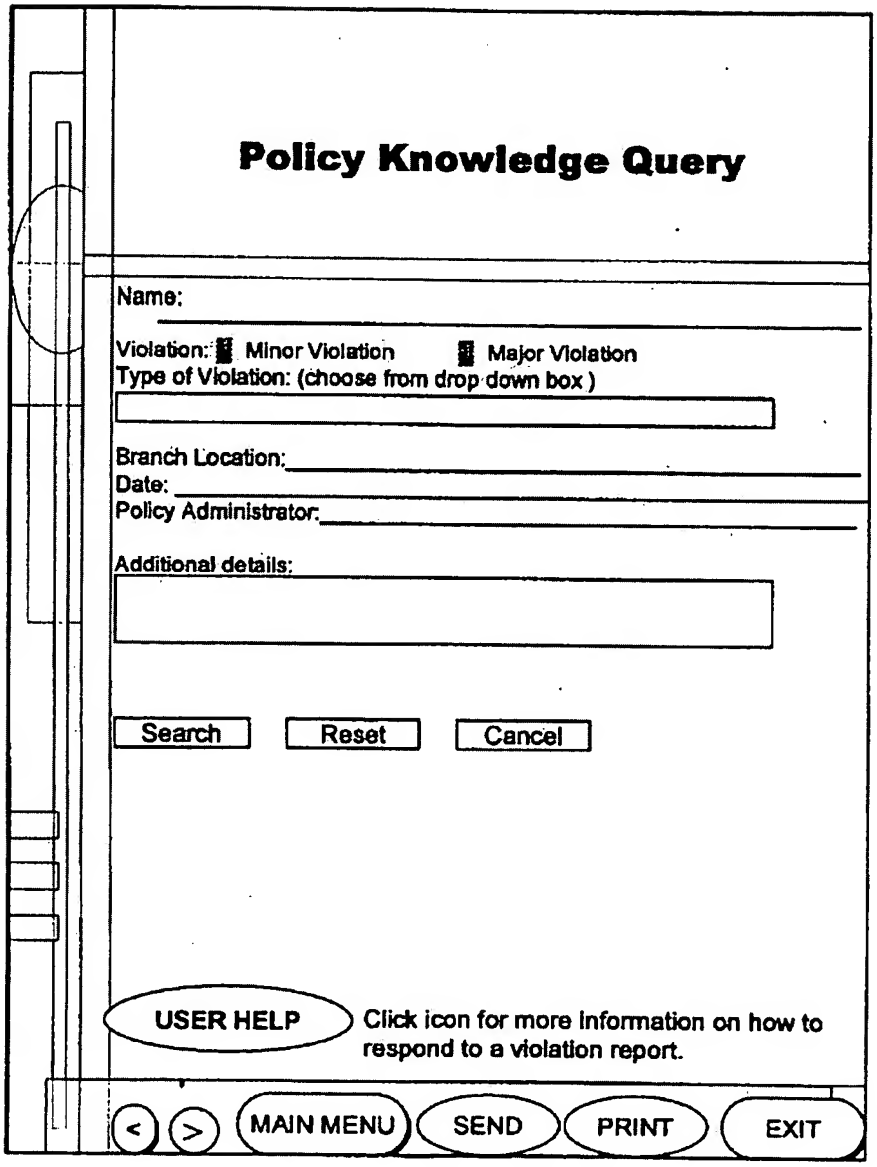


Figure 41

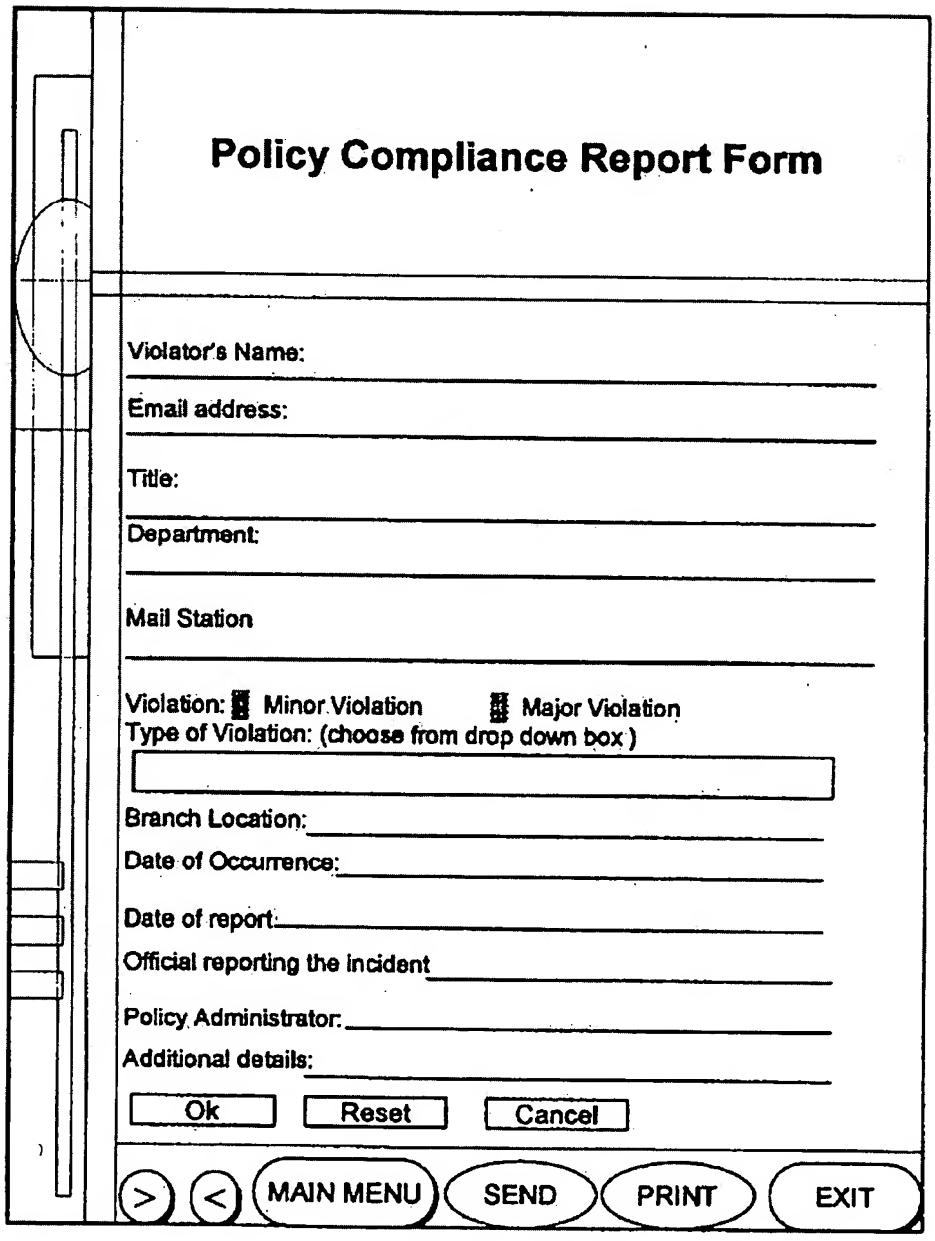


Figure 42

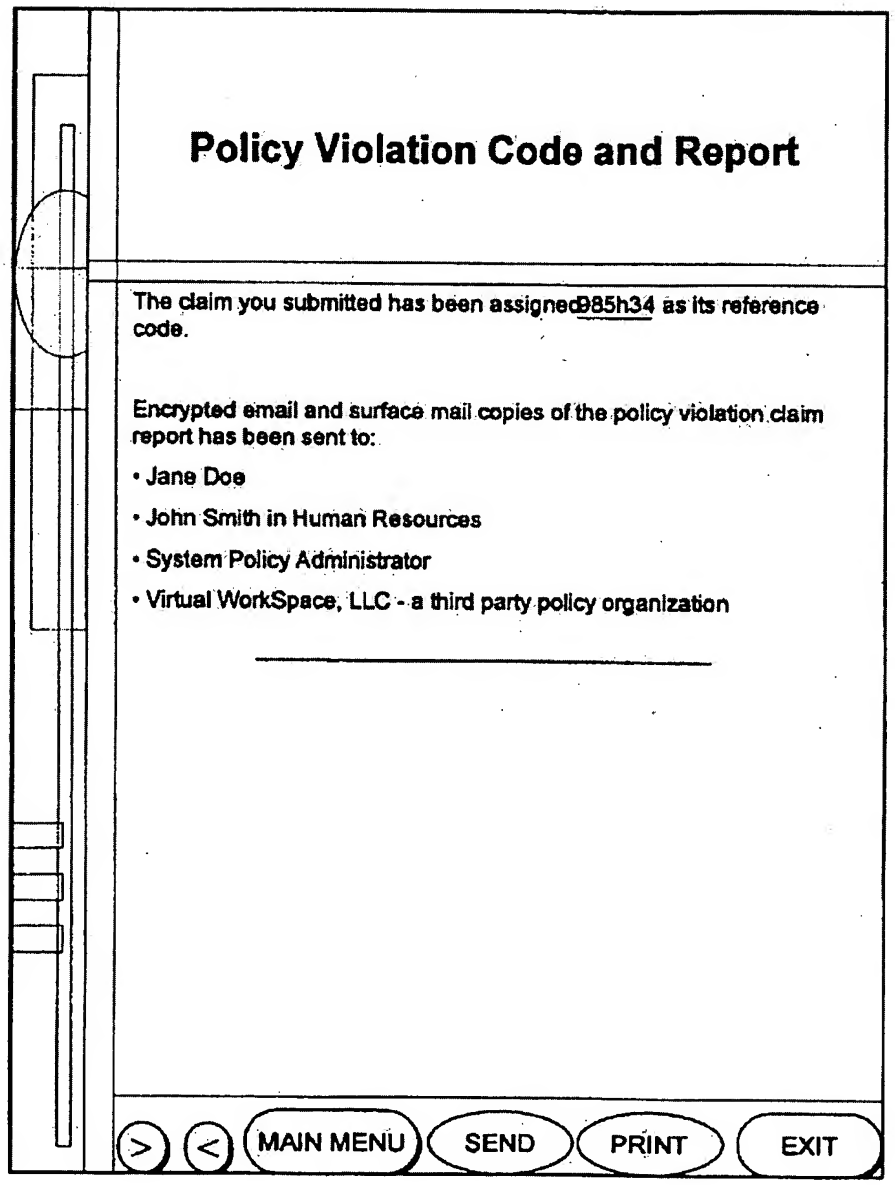


Figure 43

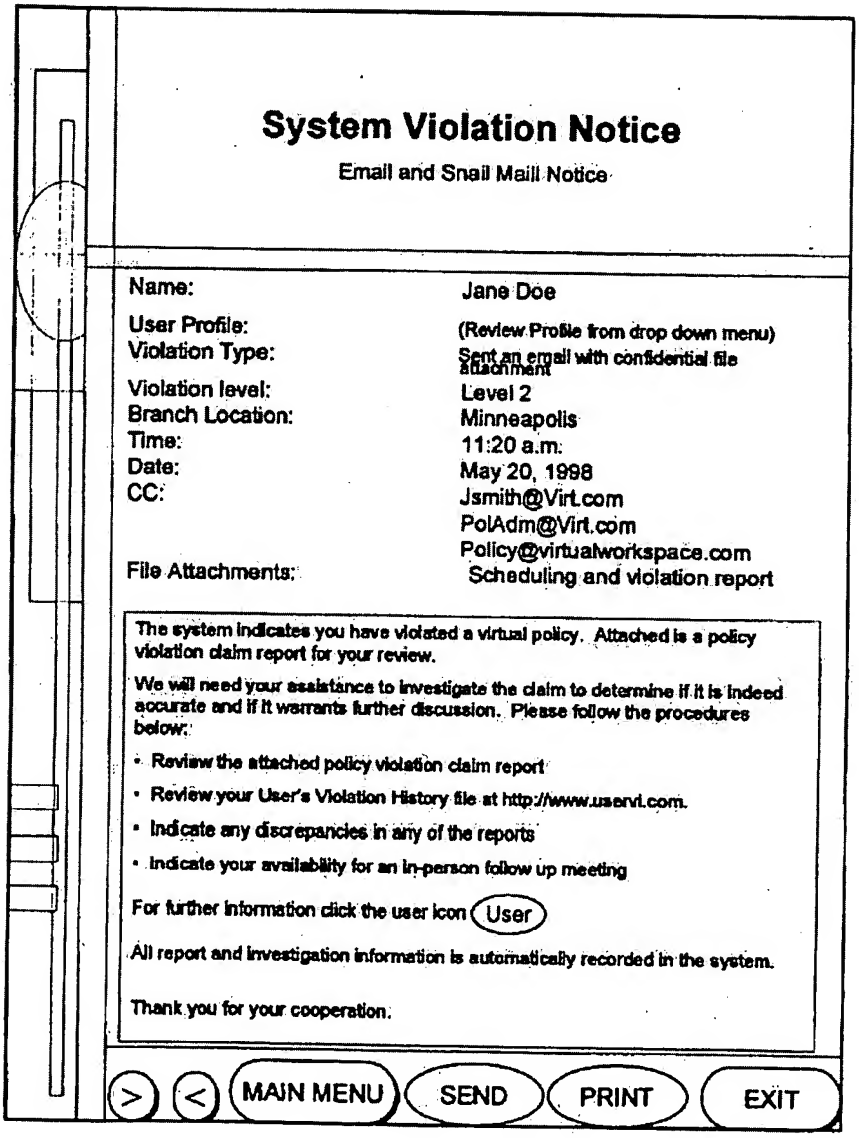


Figure 44

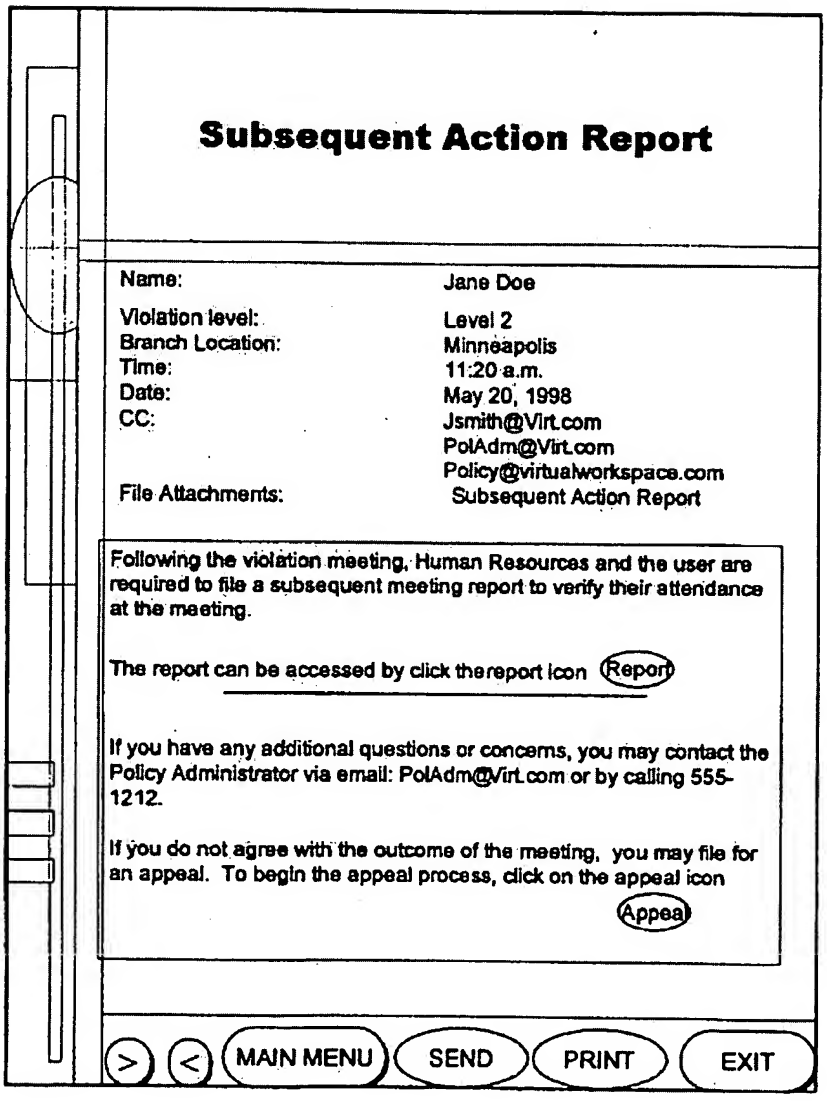


Figure 45

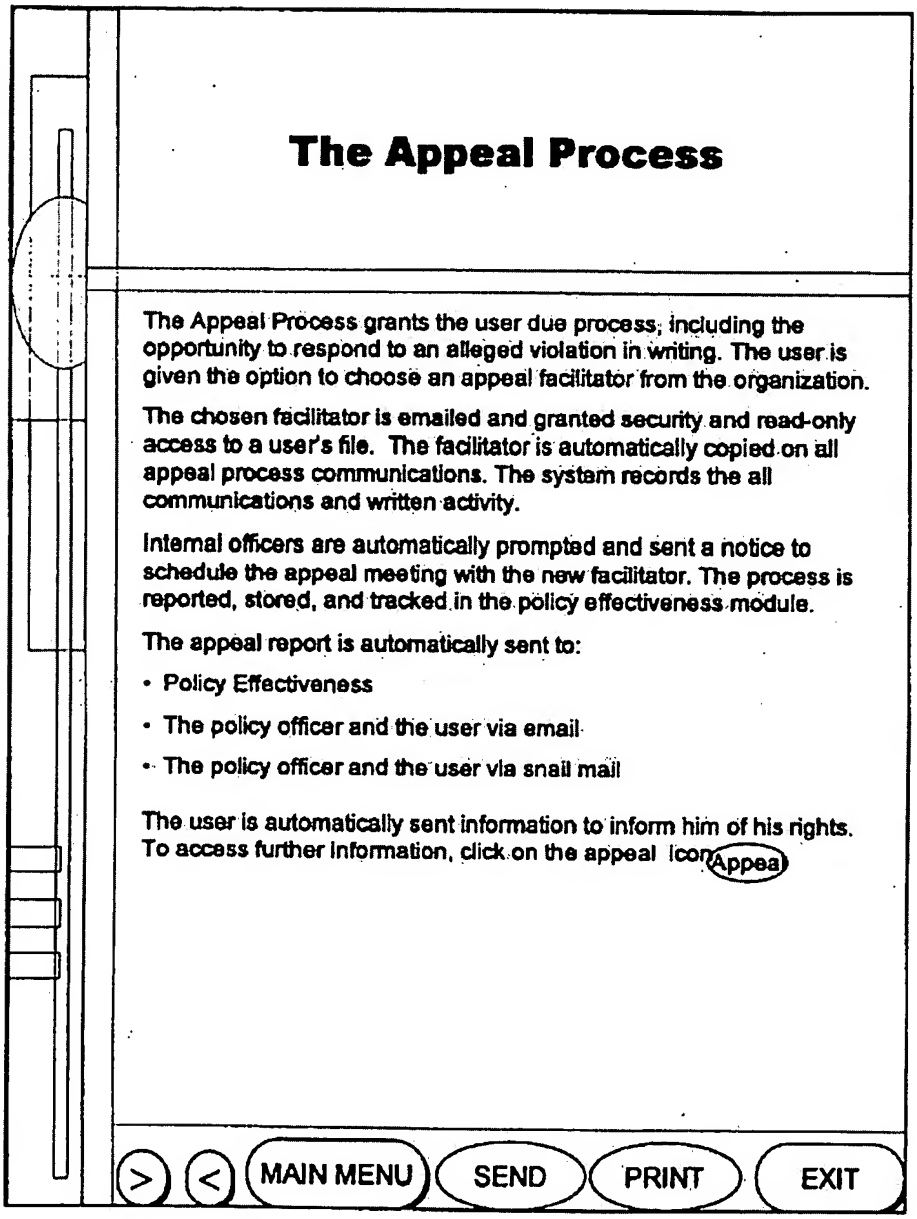


Figure 46

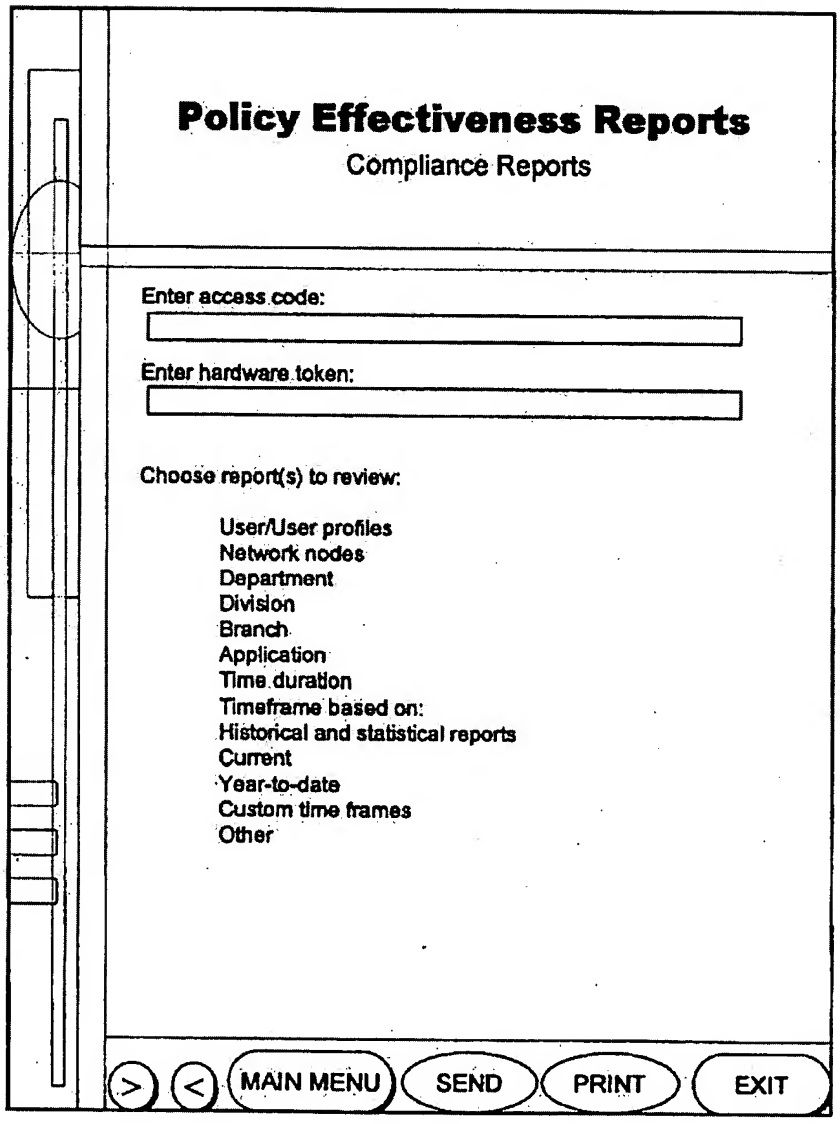


Figure 47

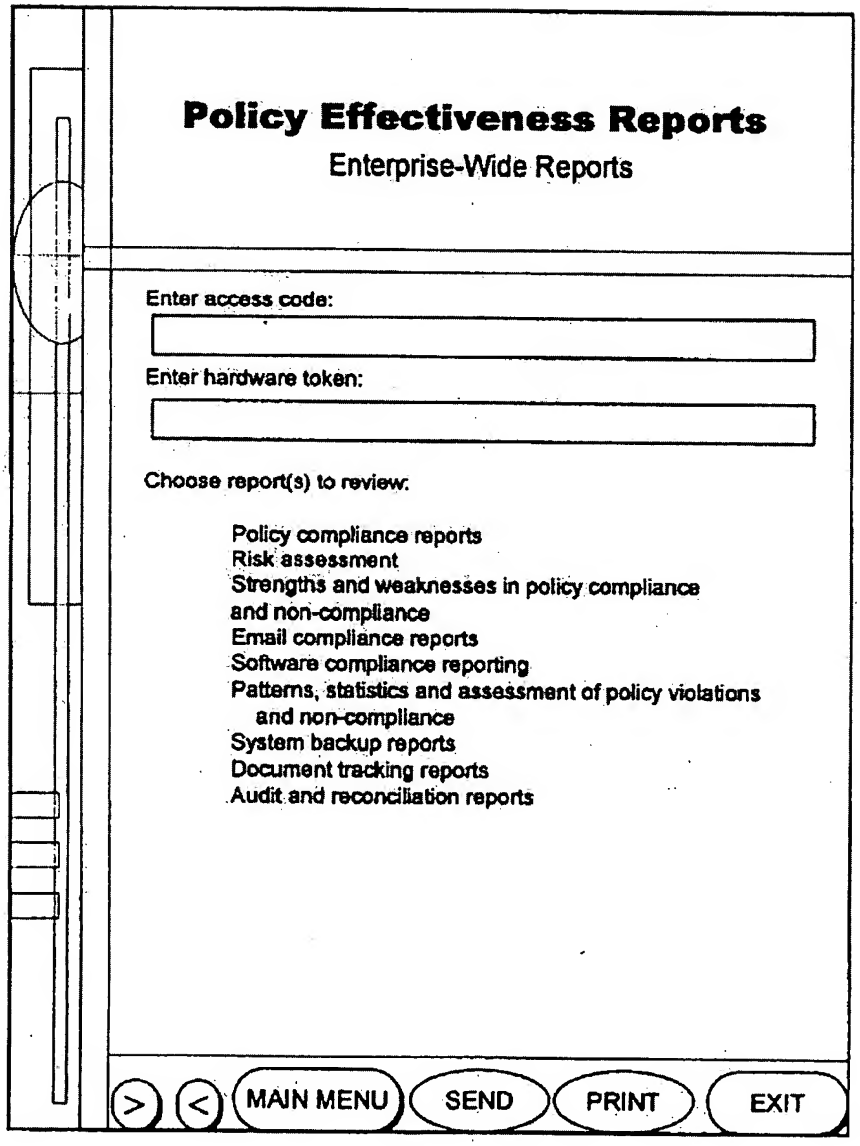


Figure 48

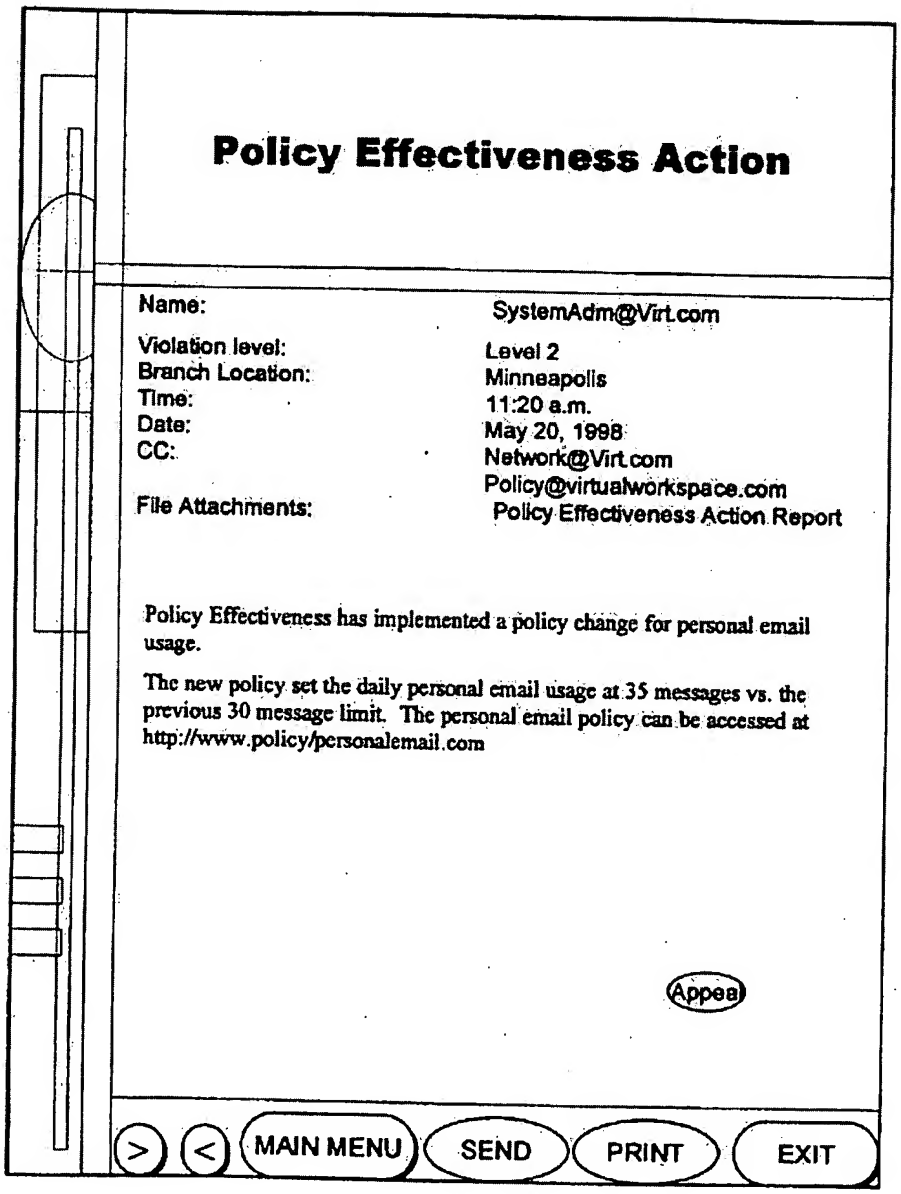
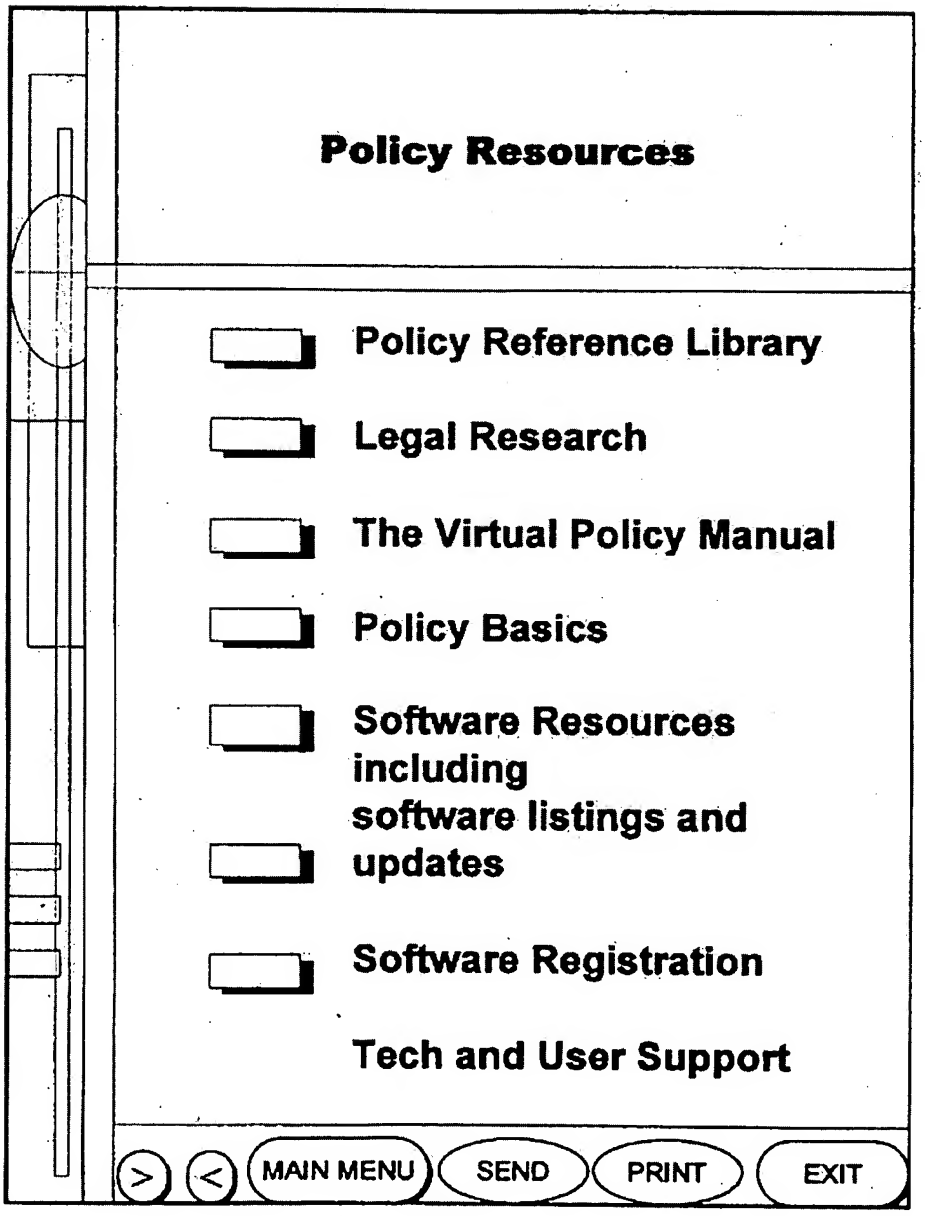


Figure 49



NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM

BACKGROUND

1. Field of the Invention

This invention relates in general to networked computing systems, and more particularly, to a system for maintaining network security policy compliance.

2. Description of Related Art

The Internet and computer networks allow organizations to store applications and information on central servers, waiting to be called up and manipulated from any location. Networks allow people greater access to files and other confidential information. Global networks, including the Internet, and remote access increase the vulnerability of corporate data, increase the risk of information leaks, unauthorized document access and disclosure of confidential information, fraud, and privacy.

Employees are the greatest threat to an organization's information security. Employees with access to information resources including email, the Internet, and on-line networks significantly increase the security risks.

Employees are using email for personal purposes creating questions of appropriate use of company resources, workplace productivity and appropriateness of message content. One of the greatest sources of information leaks is employee sent email. With electronic communication and networks, an electronic paper trail is harder to determine, since no record of who accessed, altered, tampered with, reviewed, or copied a file can make it very difficult to determine a document's authenticity, and provide an audit and paper trail. In addition, there is no automated system to centrally collect, analyze, measure, index, organize, track, determine authorized and unauthorized file access and disclosure, link hard copy information with electronic files including email, and report on how information flows in and out of an organization.

Setting proper use and security policies are a method to create order and set standards for network use. Policies are ineffective unless users understand and comply with the policies. Unfortunately, most organizations do not have tangible proof when, and if, a network-based policy violation has occurred until long after the damage has been done. Due to the technical nature of network policy violations, policy enforcement officers may not have adequate knowledge, skill, and evidence to properly execute a policy violation claim. Cases of selective policy enforcement can occur if policy violations are not consistently reported, filed, investigated, and resolved.

Employees often view e-mail as equivalent to a private conversation. This view often does not reflect the official position of the organization. These communications reflect preliminary thoughts or ideas that have not been reviewed by the organization and typically only reflect the personal opinion of the parties involved. Yet, since employees of the organization create these communications, courts and regulatory agencies have concluded that employee communications can reflect the organization's view. There is a further need for network communications software programs that offers robust policy compliance assistance, policy effectiveness monitoring and reporting.

There is a need for an automated system to assist policy enforcement officers with proper policy enforcement procedure, and methods to measure policy effectiveness, appropriateness, user system activity and compliance.

SUMMARY OF THE INVENTION

To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a method and apparatus for maintaining policy compliance on a computer network. A system in accordance with the principles of the invention performs the steps of electronically monitoring network user compliance with a network security policy stored in a database, electronically evaluating network security policy compliance based on network user compliance, and electronically undertaking a network policy compliance action in response to network security policy compliance. The network policy compliance actions may include electronically implementing a different network security policy selected from network security policies stored in the database, generating policy effectiveness reports, and providing a retraining module to network users.

One preferred embodiment of the present invention includes notifying a network user and a policy administrator, providing a retraining module to the network user, and restricting the network user's network access rights in response to monitoring network user compliance.

These and various other advantages and features of novelty which characterize the invention and various preferred embodiments are pointed out with particularity in the claims which are annexed hereto and which form a part hereof. However, for a better understanding of the invention, its advantages, and the objects obtained by its use, reference should be made to the drawings which form a further part hereof, and to accompanying descriptive matter, in which there is illustrated and described specific examples of apparatus in accordance with preferred embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a block diagram illustrating a policy effectiveness system according to an embodiment of this invention;

FIG. 2 is a block diagram illustrating the steps performed by the policy training module according to an embodiment of this invention;

FIGS. 3A–3C are block diagrams further illustrating the steps performed by a policy training module according to an embodiment of this invention;

FIG. 4 is a block diagram further illustrating the steps performed by a policy training module in administering a policy training exam;

FIG. 5 is a block diagram further illustrating the operation of a policy effectiveness system according to an embodiment of this invention;

FIG. 6 is a block diagram illustrating the steps performed by a policy compliance and reporting module according to an embodiment of this invention;

FIG. 7 is a block diagram further illustrating the steps performed by a policy compliance and reporting module according to an embodiment of this invention;

FIG. 8 is a block diagram illustrating the appeal process performed by a policy compliance and reporting module according to an embodiment of this invention;

FIG. 9 is a block diagram further illustrating a policy effectiveness system according to an embodiment of this invention;

FIG. 10 is an exemplary screen display illustrating the opening screen for policy training according to an embodiment of the invention;

FIG. 11 is an exemplary screen display illustrating the terms of the software licensing agreement according to an embodiment of the invention;

FIG. 12 is an exemplary screen display illustrating the terms of the continuation of the software licensing agreement according to an embodiment of the invention;

FIGS. 13 and 14 are exemplary screen displays illustrating the terms of the privacy agreement according to an embodiment of the invention;

FIG. 15 is an exemplary screen display illustrating the choosing a screen identity according to an embodiment of the invention;

FIG. 16 is an exemplary screen display illustrating assigning the user a session number according to an embodiment of the invention;

FIG. 17 is an exemplary screen display illustrating the introduction to the virtual facilitator according to an embodiment of the invention;

FIG. 18 is an exemplary screen display illustrating the suggested policy according to an embodiment of the invention;

FIG. 19 is an exemplary screen display illustrating the network user discussion options according to an embodiment of the invention;

FIG. 20 is an exemplary screen display illustrating group policy discussions according to an embodiment of the invention;

FIG. 21 is an exemplary screen display illustrating policy writing according to an embodiment of the invention;

FIG. 22 is an exemplary screen display illustrating the network user discussion options according to an embodiment of the invention;

FIG. 23 is an exemplary screen display illustrating the policy consensus according to an embodiment of the invention;

FIG. 24 is an exemplary screen display illustrating the policy training options according to an embodiment of the invention;

FIG. 25 is an exemplary screen display illustrating the policy exam according to an embodiment of the invention;

FIG. 26 is an exemplary screen display illustrating a training feedback and evaluation form according to an embodiment of the invention;

FIG. 27 is an exemplary screen display illustrating an Appropriate Use Agreement/Employee Agreement form according to an embodiment of the invention;

FIG. 28 is an exemplary screen display illustrating an Appropriate Use Agreement/Employee Agreement form according to an embodiment of the invention;

FIG. 29 is an exemplary screen display illustrating the end of the training according to an embodiment of the invention;

FIG. 30 is an exemplary screen display illustrating the policy compliance and reporting according to an embodiment of the invention;

FIG. 31 is an exemplary screen display illustrating the User Profile according to an embodiment of the invention;

FIG. 32 is an exemplary screen display illustrating Email Compliance according embodiment of the invention;

FIG. 33 is an exemplary screen display illustrating Document Management according to an embodiment of the invention;

FIG. 34 is an exemplary screen display illustrating Software Compliance according to an embodiment of the invention;

FIG. 35 is an exemplary screen display illustrating the audit function according to an embodiment of the invention;

FIG. 36 is an exemplary screen display illustrating Network Non-Compliance Notice according to an embodiment of the invention;

FIG. 37 is an exemplary screen display illustrating a Network Compliance Action Notice according to an embodiment of the invention;

FIG. 38 is an exemplary screen display illustrating a policy compliance violation report according to an embodiment of the invention;

FIG. 39 is an exemplary screen display illustrating a network policy action notice according to an embodiment of the invention;

FIG. 40 is an exemplary screen display illustrating a policy knowledge query according to a embodiment of the invention;

FIG. 41 is an exemplary screen display illustrating a policy compliance violation report according to an embodiment of the invention;

FIG. 42 is an exemplary screen display illustrating a policy compliance violation code and report according to an embodiment of the invention;

FIG. 43 is an exemplary screen display illustrating a System Violation Notice Email and Snail Mail Notice according to an embodiment of the invention;

FIG. 44 is an exemplary screen display illustrating a Subsequent Action Report according to an embodiment of the invention;

FIG. 45 is an exemplary screen display illustrating The Appeal Process according to an embodiment of the invention;

FIG. 46 is an exemplary screen display illustrating policy effectiveness reports according to an embodiment of the invention;

FIG. 47 is an exemplary screen display illustrating policy effectiveness reports according to an embodiment of the invention;

FIG. 48 is an exemplary screen display illustrating a policy effectiveness according to an embodiment of the invention; and

FIG. 49 is an exemplary screen display illustrating policy resources according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following description of the exemplary embodiments, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration a specific embodiment in which the invention may be practiced. It is to be understood that other embodiments may be utilized and that structural changes may be made without departing from the scope of the present invention.

The present invention provides a method and apparatus for maintaining policy compliance on a computer network.

FIG. 1 is a block diagram illustrating policy effectiveness system 100 according to an embodiment of this invention. The hardware generally implementing the policy effectiveness system 100 may include computers having processors and memories distributed over a network as is well-known

in the art. The memory may include RAM or fixed storage. The program steps implementing this invention are stored in the memory and executed by the computer processor. The present invention is may be implemented using an intranet based application that can be stored on central servers, waiting to be called up and manipulated via a Web browser from any location. Those skilled in the art will recognize that a variety of configurations can be used without departing from the scope of the present invention and that a wide variety of distributed and multi-processing systems may be used. Each of the blocks of FIG. **1** will be introduced, followed by a detailed explanation of each block.

Block **105** represents a policy training module for developing network security policies.

Block **110** represents a policy compliance monitor for monitoring compliance across the network.

Block **115** represents a policy compliance and reporting module for managing information received from the compliance monitor.

Block **120** represents the policy effectiveness module for managing the policy training module **105** and compliance monitor **110**.

Block **130** represents the database for storing policy and compliance information for the policy effectiveness system **100**.

Block **135** represents the document management system of the compliance monitor **130**.

Block **140** represents the email compliance system of the compliance monitor **130**.

Block **145** represents the policy resource module for storing and managing policy resources.

Block **150** represents the user profile module for storing user information.

Policy Training Module **105**

The policy training module **105** typically is an interactive, multimedia, policy awareness training program which helps employees gain a better understanding of the basic concepts of network security, email and Internet technologies.

The policy training module **105** presents the network user with a suggested network policy the organization wishes to implement. Policy training module **105** is designed to help the user understand potential risks that an organization faces if a policy is not implemented, the potential advantages and disadvantages of the policy in question, and the management and ethical principles affecting the potential policy in question. The network policies are generated by guidelines created from employee feedback obtained during a training session.

The policy training module **105** is comprised of several templates. When the system is first implemented, policy consultants work with management personnel within an organization to determine the organization's policies for the initial training sessions, which may relate to, for example, an entire enterprise or a specific department of an enterprise. The initial policies are entered into a policy training database **130** and are the foundation for the initial training programs. As is further described below, after the initial policy training session, the policy effectiveness system **100** will analyze all of the information gathered from the areas it monitors and compare it to each network user profile **150** to determine the policy training needs of individual network users. Then, the system customizes the policy training materials for the user training sessions.

To access policy training materials, the user is prompted to enter a password and hardware token. The user may be shown a hypertext list of policy training options. The training options may be, for example, to enter a policy training session, review for a policy exam, or take a policy exam.

Policy Training Session

The policy training session may combine interactive multimedia, group policy development discussions, and policy exercises with individual policy review and feedback screens. The result is typically employee generated policy guidelines for network security policies.

In the preferred embodiment, the computer screen for the policy training session is divided into three frames. The divided screen gives the user the option to review and answer policy recommendation questions, see and participate in group policy discussions, and pause the interactive group policy discussion session. After pausing the interactive group policy discussion section, the user may review dynamic policy recommendations and statistics from previous policy sessions, request additional information on a topic or subject presented during the previous policy session, or seek technical and product support.

The policy training module **105** collects and records both individual and group policy recommendations. The policy training module **105** uses the user's policy recommendations as a benchmark for other users to use during policy creation/training sessions, and to track policy training effectiveness.

FIG. **2** is a block diagram illustrating the steps performed by the policy training module according to an embodiment of this invention.

Block **200** represents the beginning of the policy training process. FIG. **10** is an exemplary screen display illustrating the opening screen for policy training according to an embodiment of the invention. The user may be asked to read a licensing agreement and indicate if he accepts or declines the terms of the agreement by clicking on the appropriate icon. FIG. **11** is an exemplary screen display illustrating the terms of the software licensing agreement according to an embodiment of the invention. FIG. **12** is an exemplary screen display illustrating the terms of the continuation of the software licensing agreement according to an embodiment of the invention. A message stating the privacy rights of the user typically remains on the screen until the user clicks on an accept or decline icon. FIGS. **13** and **14** are exemplary screen displays illustrating the terms of the privacy agreement according to an embodiment of the invention.

Block **202** represents the policy training module **105** presenting the network user with screen personality options. A screen personality represents a person who is executing the training session under an assumed screen name and identity. In other words, a screen relates to a real person taking a training session. The user is typically presented with a screen and is asked to choose a screen name and identity (e.g., Avatar) from a list of screen personalities for the training session. Such screen personalities give users greater privacy and the freedom to answer policy questions without fear of retaliation from other employees participating in the program. FIG. **15** is an exemplary screen display illustrating the choosing a screen identity according to an embodiment of the invention.

Block **204** represents the policy training module **105** recording the network user's screen personality in the policy effectiveness database.

Block **204** represents the policy training module **105** assigning the user a session number. FIG. **16** is an exemplary screen display illustrating assigning the user a session number according to an embodiment of the invention.

Block **206** represents the policy training module **105** recording the network user's session number. The session number may be used to track and reference the training session in the policy effectiveness module.

Block **208** represents the policy training module **105** presenting the network user with a virtual training room. The user may be prompted to click on an icon to enter the virtual training room. The virtual training room is typically similar to an Internet chat room.

Block **208** represents the policy training module **105** presenting a virtual facilitator. In a preferred embodiment, the user is introduced to the program's virtual facilitator who introduces the training participants to each other, explains the training rules, and assures the training program remains on schedule. The virtual facilitator is typically stored in the policy training database **130**. FIG. **17** is an exemplary screen display illustrating the introduction to the facilitator according to an embodiment of the invention.

In the preferred embodiment, a maximum of 5 screen personalities can participate per training session. Block **212** is a decision block representing the policy training module **105** determining if there are less than three participants registered for a session. If so, block **220** represents the policy training module **105** determining the number of virtual personalities needed for the system; otherwise, control is passed to decision block **214**. The system monitors the number of screen personalities registered for a training session. The system records each user's training session including the user's policy suggestions, individual feedback and onscreen comments provided during the training session. Block **222** the system generates a virtual personality to participate in the training session. A virtual personality may be implemented in the form of a template having fields including information copied from a user's previous training session. When the policy training module **105** determines that a virtual personality is needed for a training session, the present system may be implemented so that the module **105** launches an algorithm to generate a virtual personality to participate in the training session. The algorithm copies information from the policy recommendation database **224** stored in database **130**. Block **226** represents the policy training module **105** storing the virtual personality in the database **224**. The policy recommendation database **224** is comprised of policy information previously submitted by a screen personality including policy suggestions, individual feedback and onscreen comments provided during previous training sessions. Virtual personality information obtained during previous training session is retrieved from the policy recommendation database **224**. The algorithm copies the policy information from the previous policy modules, positions and scripts the policy information for the present training session. Script is defined as positioning and pacing the policy information per policy module to make it appear as though it is occurring in real-time. This provides the user with a virtual personality and an interactive, simulated real-time training experience without the user being dependent upon the availability of others for interaction, discussions and training. After introductions, the user is typically prompted to click on either an agree or decline icon to indicate his understanding of the training rules and to indicate his readiness to proceed. Block **220** represents the policy training module **105** generating a policy.

Block **214** is a decision block representing the policy training module **105** determining if there are less than five screen personalities registered for the session. If so, block **216** represents the policy training module **105** dividing the participants into two sessions; otherwise, control is passed to block **220** which represents the policy training module **105** generating a policy. Block **216** represents the policy training module **105** assigning the participants a new session number.

The Policy Training Process:

FIGS. **3A–3C** are block diagrams further illustrating the steps performed by the policy training module **105** in performing the generating a network security policy step represented by block **220** according to an embodiment of this invention;

Block **300** represents the policy training module **105** indicating that the network user is ready to begin policy training by presenting the network users with suggested policy information.

Block **302** represents the policy training module **105** receiving suggested policies from the network users. FIG. **18** is an exemplary screen display illustrating the suggested policy according to an embodiment of the invention. The suggested policy information typically is stored in a policy training database **130**. The user is asked to review the policy information and a policy suggestion for a limited period of time. The policy training module **105** collects a policy suggestion from each network user's policy review session.

Block **304** represents the policy training module **105** recording all individual policy recommendations.

Block **306** represents the policy training module **105** prompting the network user to join a group discussion after the network user has reviewed the information on his own. The network user indicates his readiness to join the group discussion, such as by clicking an icon. The network user's signal may be sent to the other participants' screens. FIG. **19** is an exemplary screen display illustrating the network user discussion options according to an embodiment of the invention.

Block **308** represents the policy training module **105** notifying the other participants that a network user is prepared to enter the group session. Once the individual network users are ready to discuss the policy, the facilitator begins the session monologue and monitors the session's content and time.

Block **310** represents the policy training module **105** retrieving the electronic facilitator from the database **120**. The electronic facilitator serves as a moderator for the training module. For example, the electronic facilitator prompts the users for input and monitors the time spent on each issue.

Block **312** represents the policy training module **105** connecting individual network users to the policy training chat room.

Blocks **314, 316** and **318** represent the individual network user computers connected to the policy chat room of the policy training module **105**. One or more individual network user's policy recommendations may be displayed to the group.

Block **322** represents the policy training module **105** displaying network user policy recommendation to the group. The policy recommendations may be shown in a different color and font. FIG. **20** is an exemplary screen display illustrating group policy discussions according to an embodiment of the invention. The individual recommendations are used to develop a group policy consensus.

From the discussion, the group confers, online, to write a policy recommendation. All group participants can view the policy recommendations and group discussions from previous policy training sessions. FIG. **21** is an exemplary screen display illustrating policy writing according to an embodiment of the invention.

Block 324 is a decision block representing the policy training module 105 querying the user regarding whether he wants more policy information. If so, block 326 represents the policy training module 105 retrieving the policy training information and displaying it to applicable network users; otherwise block 328 represents the policy training module 105 collecting policy recommendations from the group. The group confers, online, to write a policy recommendation. The policy training module 105 collects and records all group policy recommendations. FIG. 22 is an exemplary screen display illustrating the network user discussion options according to an embodiment of the invention.

Block 330 represents the policy training module 105 recording the group policy recommendations in the policy recommendation database 224.

Block 332 represents the policy training module 105 calculating and ranking the group responses in the policy training database. For example, the policy with the most user votes may be the policy of group consensus.

Block 334 is a decision block representing the policy training module 105 determining if a policy consensus has been achieved. If so, then block 336 represents the policy training module 105 displaying the group consensus; otherwise, control typically is returned to block 322. If there is a tie for group consensus, the system requires network users to review the policy options and re-vote. Each user's policy information is displayed the group reconsiders their recommendations and attempts to come to a group policy consensus.

The process illustrated in blocks 322 through 334 is repeated until a group policy consensus is achieved.

Block 336 represents the policy training module 105 displaying policy consensus. FIG. 23 is an exemplary screen display illustrating the policy consensus according to an embodiment of the invention.

Block 338 represents the policy training module 105 recording the policy consensus. The process of developing a consensus policy is repeated until all of the policy modules have been reviewed and addressed.

Block 340 is a decision block representing the policy training module 105 determining if there are no additional policy modules to complete.

If so, block 300 represents a repeat of the policy generation process; otherwise, block 342 represents the policy training module 105 presenting a suggested policy to the network user and assembling and recording the group consensus policies from each policy module.

The policy training module 105 assembles and records the group consensus policies from each policy module in the network security policy database 130.

Block 344 represents the end of the policy generation process of the policy training module 105.

When the training session is completed, the network user is given the options to start the policy exam, review policy training materials, or end the session. FIG. 24 is an exemplary screen display illustrating the policy training options according to an embodiment of the invention.

Start the Policy Exam

FIG. 4 is a block diagram further illustrating the steps performed by the policy training module in administering a policy training exam according to an embodiment of the present invention. The network user is given an online policy exam to reinforce the information presented in the policy training session.

Block 400 represents the policy training module 105 receiving a request for a policy training exam from the network user.

Block 402 represents the policy training module 105 retrieving a policy exam from the policy training database 130 and presenting it to the network user. FIG. 25 is an exemplary screen display illustrating the policy exam according to an embodiment of the invention. Once the network user completes the exam, he is prompted to send the exam to policy effectiveness 120 where the information regarding the user's taking of the exam is recorded.

Block 404 represents the policy training module 105 receiving the exam answers from the network user and tabulating the network user's score. During the exam tabulation period, the network user is asked to fill out a policy training feedback and evaluation form.

Block 406 represents the policy training module 105 retrieving a policy training feedback and evaluation form from the policy training database 130 and sending it to the network user. FIG. 26 is an exemplary screen display illustrating a training feedback and evaluation form according to an embodiment of the invention. The network user completes the policy training feedback and evaluation form and returns it to the policy training module 105.

Block 408 represents the policy training module 105 storing the policy training feedback and evaluation form in the User's Profile database 150.

Block 410 represents the policy training module 105 sending the network user his exam score after the feedback and evaluation form is completed.

After the employee completes the policy building session, the policy training module 105 may request that the user sign an Appropriate Use Agreement/Employee Agreement designed to limit the organization's liability. FIG. 27 is an exemplary screen display illustrating an Appropriate Use Agreement/Employee Agreement form according to an embodiment of the invention. FIG. 28 is an exemplary screen display illustrating an Appropriate Use Agreement/Employee Agreement form according to an embodiment of the invention. Block 412 represents the policy training module 105 sending the network user an Appropriate Use Agreement/Employee Agreement. The user reads and signs the Agreement. The user returns the Agreement to the policy training module 105. The signed Agreement is kept in the User Profile database 200 and a copy is emailed to the user for his records.

Block 414 represents the policy training module 105 receiving the Agreement and storing it in the User Profile 150.

Block 416 represents the policy training module 105 sending an email message to the network user with a copy of the Agreement attached.

Block 418 represents the end of the policy exam process. FIG. 29 is an exemplary screen display illustrating the end of the training according to an embodiment of the invention. If the user fails the exam, the policy training module 105 will ask him if he wants to retake the exam, review policy training materials, or end the session.

Policy Compliance Monitor 110

The Policy Compliance Monitor 110 works with the Policy Effectiveness Module 120 to provide network user compliance monitoring with network security policy stored in a database, it electronically evaluates network security policy compliance based on network user compliance, and undertakes a network policy compliance action in response to network security policy compliance. Network user compliance monitoring is defined as monitoring network activity to insure users are in compliance with the organization's network security policies. Network security policy is a set of rules designed to limit an organization's risk and liability.

FIG. 5 is a block diagram further illustrating the operation of the policy effectiveness system according to an embodiment of this invention.

The policy compliance monitor oversees user profile, email compliance, internet compliance, document management and software compliance functions to collect network user security policy compliance activities. FIG. 30 is an exemplary screen display illustrating the policy compliance and reporting according to an embodiment of the invention.

Block 110 represents the policy compliance monitor of the policy effectiveness system 100.

Block 150 represents the user profile module of the policy effectiveness system 100. The user profile module 150 is a database comprised of information about network users. For example, the user profile module 150 may contain information about network user policy compliance history, employment history, and network identification information. FIG. 31 is an exemplary screen display illustrating the User Profile according to an embodiment of the invention.

Block 140 represents the email compliance module of the policy effectiveness system 100. The email compliance module 140 collects information on network users' email use activity. FIG. 32 is an exemplary screen display illustrating email compliance according to an embodiment of the invention.

Block 135 represents the document management module of the policy effectiveness system 100. FIG. 33 is an exemplary screen display illustrating Document Management according to an embodiment of the invention. The document management module 135 collects information on documents in the system. This may include document history, document authenticity, network user access to documents, and document access and disclosures.

Block 500 represents the software compliance module of the policy effectiveness system 100. The software compliance module 500 collects information on how network users utilize software on the network. FIG. 34 is an exemplary screen display illustrating Software Compliance according to an embodiment of the invention.

Block 502 represents the audit function of the policy effectiveness system 100. The audit function collects information from all of the policies monitored by the policy compliance monitor 110. Each monitored policy is assigned a value representing a target baseline compliance level for network policy compliance ("network policy compliance"). In the preferred embodiment, the numeric value assigned to each monitored policy is 95, representing that for each policy 95% user compliance is required. Each network user compliance activity has a numeric value the system monitors representing a target baseline compliance level for user policy compliance ("user policy compliance").

Block 504 represents the network security policy compliance database of the database 130. The baseline compliance level assigned to each monitored policy is stored in the network security policy compliance database 504 of the database 130. The audit function is responsible for reviewing network user compliance and network security policy.

FIG. 35 is an exemplary screen display illustrating the audit function according to an embodiment of the invention. Block 506 represents the network security policy database. The network compliance value is monitored in relation to the user compliance value stored in the network security policy database 506.

Block 508 is a decision block representing the policy effectiveness system 100 analyzing the network policy compliance value in relation to the user compliance policy value. If the user policy compliance value is greater than or equal to the network policy compliance value, then block 120 represents the policy effectiveness system notifying the policy effectiveness module 120 that the network is in compliance. Otherwise, if the network policy compliance value is greater than the user policy compliance value, the policy compliance monitor 110 measures the difference between the network policy compliance value and the user policy compliance value and undertakes a network compliance action in response to that difference. Alternatively, the policy compliance monitor could undertake a network a compliance action anytime a policy violation occurred.

FIG. 36 is an exemplary screen display illustrating Network Non-Compliance Notice according to an embodiment of the invention. Each policy is associated with a corresponding group of network policy compliance actions ranging from a mild (e.g., notifying a network user), level two (e.g. notifying the network user and a policy administrator), level three (e.g., providing a retraining module to a network user, restricting a network user's network access rights) and a level four action (e.g., restricting the network user's network access rights.) Each compliance action in the group is assigned a value related to a numeric value that may be reported from monitoring network user compliance. The numeric value assigned is based on the severity of the network policy compliance violation, i.e: the difference between the network policy compliance value and the user policy compliance value.

Upon recording the difference between the network policy compliance value and the user policy compliance value, the policy compliance and reporting module 115 records this information in the network security policy database 506 and begins undertaking the appropriate network compliance action.

For example, an organization may have a personal email use policy. The personal email use policy may limit each user to sending a maximum of 20 personal email messages per day. The system assigns the numeric value of 95 to the personal email messages policy. A value of 100 is the optimum network policy compliance value. The compliance monitor collects information on network user compliance for personal email use. If an individual sends 25 email messages, the system records a user policy compliance value of 90. The user policy compliance value of 90 is compared to the network policy compliance value of 100. The difference of 5 (95−90) indicates to the policy effectiveness system 100 that a network policy compliance action may be taken. In this example, a network user compliance value of 5 may tell the system to execute a network compliance action.

In the preferred embodiment, the system has four action levels. Each action level may be undertaken in response to a range of differences in compliance values. FIG. 37 is an exemplary screen display illustrating a Network Compliance Action Notice according to an embodiment of the invention.

At a first action level, the system may send an email notifying the network user to cease and desist the non-compliant activity.

At a second action level, the system may prompt the system administrator to follow screen prompts to initiate procedures for the infraction. The policy effectiveness system 100 notifies the network user and a system administrator. Email and surface mail are automatically sent to the alleged violator and the system administrator. The message may ask the alleged violator to discontinue the inappropriate

behavior or to reread the Intranet-base Policy Manual. The policy effectiveness system **100** records if the user visits the electronic site of the Policy Manual.

At a third action level, the policy effectiveness system **100** may file a policy violation report and launch an investigation. The policy effectiveness system **100** sends email and surface mail to the alleged violator and the system administrator informing them of the violation. A policy retraining module may be the most likely course of action. At the third action level, the actions of the second infraction are initiated and additionally an immediate referral is made to the appropriate policy officer for review and action.

At the fourth action level, the policy effectiveness system **100** may restrict the network user's network access rights and prompt the system administrator to either begin investigation procedures and/or initiate a signal to the policy knowledge base to determine the recommended course of action.

Block **510** represents the policy effectiveness system **100** undertaking a network policy compliance action. The policy effectiveness system **100** sends a signal to policy compliance and reporting **115** to record the non-compliant network user activity.

Policy Compliance and Reporting **115**

The policy compliance and reporting module **115** provides automated policy monitoring, policy violation procedures and reporting, it tracks policy investigations and generates policy investigation reports. These procedures work in conjunction with existing policy compliance reporting, discipline and grievance procedures to uphold the organization's technology policies.

Compliance

The policy compliance and reporting **115** monitors and records user and network system activities audit procedures and reporting, policy violation procedures/investigations/reporting, compliance/non-compliance status reporting.

FIG. **6** is a block diagram illustrating the steps performed by a policy compliance and reporting module according to an embodiment of this invention.

The policy compliance and reporting process begins when the policy compliance and reporting **115** receives a signal from the compliance monitor **110** that a network compliance action has been taken. Block **510** represents that a network compliance action has been taken by the policy effectiveness system **100**.

Block **600** represents the policy compliance and reporting **115** sending an email or pager message to the system administrator notifying the administrator that a network user compliance violation has occurred. The email message attaches a policy compliance violation report (file) to the email and instructs the system administrator to follow the compliance reporting procedures. FIG. **38** is an exemplary screen display illustrating a policy compliance violation report according to an embodiment of the invention. The email instructs the system administrator to log into the system, present a password and hardware token to access the policy violation reporting procedures and indicates the screen option to choose. The screen options available to the system administrator may include: file a policy compliance violation report, investigate a policy compliance violation report, review audit and system reports, the appeal process, review a user profile, policy resources, and policy effectiveness reports.

File a Policy Violation Report

In a preferred embodiment, a screen is displayed to the system administrator indicating a network user policy compliance violation has occurred and a network user compliance action, level two or greater, has been taken. The system administrator is instructed to click on an icon to access the network user policy compliance violation information and document the violation. FIG. **39** is an exemplary screen display illustrating a network policy action notice according to an embodiment of the invention.

Block **503** represents the policy compliance and reporting **115** retrieving the network user policy compliance violation documentation from the policy effectiveness module **120**. Policy compliance and reporting **115** advises the system administrator on how to execute the designated network user compliance violation reporting procedures. This is achieved by prompting the system administrator through the reporting process and presenting a policy knowledge base. FIG. **40** is an exemplary screen display illustrating a policy knowledge query according to an embodiment of the invention. A support icon is also available if the user needs to discuss a specific procedure with a Policy Consultant.

Block **604** represents the policy knowledge database of the policy compliance and reporting **115**. The policy knowledge database is comprised of automated network user policy compliance violation documentation. This may include network policy violation report forms, detailed reporting instructions, and investigation procedures checklist. The policy compliance and reporting **115** analyzes the network user policy compliance violation information from the policy knowledge database **604** and determines if an investigation action is needed.

After the system analyzed the violation information, a policy violation investigation report form is displayed on the user screen. FIG. **41** is an exemplary screen display illustrating a policy compliance violation report according to an embodiment of the invention. All reports are documented in read-only format and all modifications and changes to the non-compliance reports are an addendum to the initial report. The system administrator is asked to supply the following network compliance violation information regarding the claim including the network user's name: E-mail address, title, department, mail station, type of violation (non-compliance drop down box), date of occurrence, date of report, and official report of the incident (MIS, the user, or policy officer).

A code is assigned to the policy compliance violation report. FIG. **42** is an exemplary screen display illustrating a policy compliance violation code and report according to an embodiment of the invention. Block **606** represents the policy compliance and reporting **115** assigning a code to the policy compliance violation report. The code is used to identify and track the policy compliance violation report in the policy effectiveness database. The system administrator, the policy officer and the network user are the parties that may access the policy compliance violation report. To access the policy compliance violation report the system administrator, the policy officer and the network user are given the access code to the report and are registered in the system. While completing the report, the system administrator can access a network user's policy compliance report to review their network activity history. All report communications, including the policy compliance violation report, may automatically be sent via encrypted e-mail to a third party organization and are kept in escrow. This insures the organization cannot access the policy compliance reports in the system to change the content of the reports and insure that they follow due process procedures.

The system administrator may contact the policy officer to schedule an in-person appointment with the network user.

Block 608 represents the policy compliance and reporting 115 recording the appointment. Block 610 represents the policy compliance and reporting 115 scheduling the appointment. A hyperlink to a scheduling module is activated. An example of a schedule module is Microsoft's Schedule Plus. Several meeting options are listed on the violation report to be e-mailed and surface mailed to the network user. FIG. 43 is an exemplary screen display illustrating a System Violation Notice Email and Snail Mail Notice according to an embodiment of the invention. The system monitors and records the reporting and investigation process in the policy effectiveness database.

All registered parties are automatically e-mailed the policy compliance violation report, all correspondence related to the report and the appointment date. Block 508 the report information is distributed. Copies of policy compliance violation report is automatically sent to policy effectiveness, e-mailed to policy officer, surface mailed to the network user, e-mailed to the network, and surface mail copy printed and sent to the network user. The surface mail and e-mail reports are form letters that may include an Internet address to help inform the network user about the policy compliance violation reporting process. Policy compliance and reporting 115 tracks and monitors the status of the complaint by monitoring the scheduling module and tracking where the report is in the system. Block 612 represents the policy compliance and reporting 115 distributing the policy compliance violation report information.

Printed copies of the policy compliance violation report, correspondence; and related documents have a watermark printed in the header of the print out of the policy compliance violation report with the words "corporate record" printed on the top corner of the document. The printout may include the date the document was created, who created the document, the version number of the report and the file path. This is used to insure the authenticity of the policy compliance violation report.

Subsequent Action Report

FIG. 7 is a block diagram further illustrating the steps performed by the policy compliance and reporting module 115 according to an embodiment of this invention in generating a subsequent action report. FIG. 44 is an exemplary screen display illustrating a Subsequent Action Report according to an embodiment of the invention. Block 700 represents the policy compliance and reporting module 115 receiving a message from the schedule module to begin subsequent action procedures. The policy officer, the system administrator and the network user are automatically reminded via email of the requirement to individually file subsequent meeting reports with the system. Block 702 represents the policy compliance and reporting module 115 distributing notices via email. The policy officer, system administrator and the network user are required to present login and password/token information to file subsequent action reports with the system and to verify a policy compliance violation meeting occurred.

The network user is also asked to sign an agreement indicating he attended the policy enforcement meeting and reviewed the policies of the organization. The system administrator and policy officer are asked to confirm and document that the meeting took place. All parties are complete the forms. Block 704 represents the policy compliance and reporting module 115 retrieving subsequent action reports from the parties. The system stores the documents in the policy effectiveness database.

The system administrator is prompted by the system to confirm in the subsequent action report form. The subsequent action form indicates if the network user policy compliance violation claim is still under investigation, pending or is closed.

Block 706 represents the policy compliance and reporting module 115 storing information related to the subsequent action reports. The policy compliance and reporting module 115 monitors the status of all network user compliance violations to insure that violation reports are properly reported and managed.

The Appeal Process:

FIG. 8 is a block diagram illustrating the appeal process performed by a policy compliance and reporting module according to an embodiment of this invention. FIG. 45 is an exemplary screen display illustrating The Appeal Process according to an embodiment of the invention. After filing the subsequent action report, the system gives the network user the opportunity to respond to appeal the network compliance violation. Block 800 represents the policy compliance and reporting module 115 prompting network user with the appeal option. Block 802 represents the policy compliance and reporting module 115 receiving a signal to begin appeal process. The network user is given the option of choosing an appeal facilitator from the organization. Appeal facilitators are employees of the organization randomly chosen by the system to act a facilitator for the appeal process. The policy compliance and reporting module 115 reviews network user profiles and chooses the network users with the lowest network user policy compliance violation records to be facilitator candidates. Block 804 represents the policy compliance and reporting module 115 retrieving appeal facilitator information from the policy compliance and reporting database. The user chooses the facilitator from the Appeal screen. The system records the process and automatically sends an email to the facilitator. Block 806 represents the policy compliance and reporting module 115 recording the facilitator. Block 808 represents the policy compliance and reporting module 115 assigning a password to the facilitator. Block 810 represents the policy compliance and reporting module 115 sending an email to the facilitator. The e-mail explains the appeals process to the facilitator and provides the facilitator with the passwords needed to access to the network user policy compliance violator's file. The facilitator has read-only access to the network user compliance violation reports. The facilitator is automatically copied on all appeal process communications. The system records this activity and stores it in the policy effectiveness database.

Next, the internal officers are automatically prompted and sent a notice to schedule the appeal meeting with the new facilitator, the network user, the system administrator and the policy officer. Block 812 represents the policy compliance and reporting module 115 prompting users to schedule an appeal meeting. The process is reported to, stored, and tracked in the policy effectiveness module. Block 814 represents the policy compliance and reporting module 115 the system recording the process. The appeal report is automatically sent to internal policy officers. The network user is automatically sent information to inform him of his procedural rights. The appeal report is automatically sent to the policy effectiveness module, the policy officer and the network user, and a surface mail is sent to the policy officer and the violator. Block 816 represents the policy compliance and reporting module 115 distributing appeal information to all parties.

The facilitator logs into the system and reviews all of the documents regarding the policy violation. The facilitator, the policy officer and the suspected violator meet to listen to the violator's appeal. The facilitator and the policy officer are

required to present login and password/token information to file appeal reports and to verify an appeal meeting occurred. Block **818** represents the policy compliance and reporting module **115** retrieving appeal report forms from policy compliance and reporting database. The appeal reports are comprised of several fields. The facilitator and the policy officer are required to complete the online reports. The policy effectiveness analyzes the appeal reports to determine the final decision. Block **820** represents the policy compliance and reporting module **115** analyzing the appeal reports. An email is sent to all parties with the final decision file attached. Block **822** represents the policy compliance and reporting module **115** distributing the final appeal decision. Block **824** represents the policy compliance and reporting module **115** transferring the appeal information to the policy effectiveness module **120**.

Policy Effectiveness 120

The policy effectiveness module **120** electronically collects, records, analyzes and stores information from policy compliance monitoring, analyzes policy compliance and reporting, evaluates network policy compliance actions undertaken in response to the network security policy violations and electronically implements a different network security policy selected from network security policies stored in a policy database.

The policy effectiveness module **120** analyzes information collected from the policy compliance and reporting **115** to determine if network user compliance policies are effective. FIG. **46** is an exemplary screen display illustrating policy effectiveness reports according to an embodiment of the invention FIG. **47** is an exemplary screen display illustrating policy effectiveness reports according to an embodiment of the invention. If a policy is determined to be ineffective, a new policy may need to be implemented.

The policy effectiveness module **120** monitors the policy compliance actions taken over a period of time. At the time the system is implemented, the system administrator may set the system to measure network compliance actions that have been undertaken on a monthly, quarterly, annual, historic (e.g., year-to-date) basis. After the monitoring time period has been recorded in the system, the system administrator may record the number of network policy compliance actions, per network compliance policy, considered acceptable during a said period of time.

The policy effectiveness module **120** analyzes the policy compliance actions stored in the policy compliance and reporting module **115**. Each policy is assigned a value representing a target baseline compliance level for network policy compliance ("network policy compliance"). In the preferred embodiment, the numeric value assigned to each monitored policy is 95, representing that for each policy 95% user compliance is required. The level of user compliance for a group of network users with respect to a particular policy is monitored. The network user compliance activity for a group has a numeric value, the system monitors representing the degree of group user policy compliance ("group user policy compliance"). The network compliance value is monitored in relation to the user compliance value stored in the network security policy database **506**.

FIG. **9** is a block diagram further illustrating a policy effectiveness system according to an embodiment of this invention.

Block **900** represents the policy effectiveness module **120** determining network policy compliance. Block **910** represents the policy effectiveness module **120** determining group user compliance. Block **920** is a decision block representing the policy effectiveness module **120** analyzing the network policy compliance value in relation to the group user compliance policy value. If the group user policy compliance value is greater than or equal to the network policy compliance value, then block **940** represents the policy effectiveness module **120** recording that the network is in compliance with respect to a policy. Otherwise, if the network policy compliance value is greater than the group user policy compliance value, the policy effectiveness module **120** measures the difference between the network policy compliance value and the group user policy compliance value and may undertake a network compliance action in response to that difference.

Each compliance action in the group is assigned a value related to a numeric value that may be reported from monitoring network user compliance. The numeric value assigned is based on the severity of the network policy compliance violation, i.e. the difference between the network policy compliance value and the group user policy compliance value. Upon recording the difference between the network policy compliance value and the group user policy compliance value, the policy effectiveness module **120** records this information in the network security policy database **130** and begins undertaking the appropriate network compliance action. This action may include electronically implementing a different network security policy selected from network security policies stored in the database, generating policy effectiveness reports, and providing a retraining module to network users.

For example, the system administrator may have indicated that the password policy can not have more than 5 network compliance action occur per month. If the network compliance action is greater than 5 actions per month, the system sends a message to retrieve a different policy from the database **130**. The policy selected based on indexing criteria and on the difference between the group user policy compliance and the network policy compliance values. Each policy has several actions ranging from lenient to restrictive. The policy effectiveness module **120** reviews the information collected by policy effectiveness to determine which policy to modify and the action to take. The policy effectiveness module **120** records the policy change and sends an email message to the system administrator to confirm the policy changing process. FIG. **48** is an exemplary screen display illustrating a policy effectiveness action according to an embodiment of the invention. An enterprise wide email is also sent to all network users to alert them to the change in policy.

Policy Resources 145

The policy effectiveness system **100** includes a policy resources **145** database and software resources database to help users and administrators maintain policy compliance. FIG. **49** is an exemplary screen display illustrating policy resources according to an embodiment of the invention. Materials included in the policy resources database **145** include a policy reference library, legal research, a policy manual, a and a self-serve policy section. The policy reference library has a search engine to help the user quickly search and find policy information. Users can contact support personnel either by email, page, telephony, fax, or telephone. It is important that users have immediate access to a support person, since major policy violations may require organizations to act quickly in order to protect their network from damage. Internal legal and policy personnel can access legal statutes and other related policy documen-

tation relating to email and virtual policies in the workplace. The policy manual is presented to users such that they will be able to read and review the policy manual periodically. Users are periodically required to sign an online form indicating he or she has read the policies, and any policy revisions, and understands all of policies. Annual updated information will be highlighted for fast review. The policy effectiveness system **100** tracks users visit to the policy. The self-serve policy section allows the policy officer to revise the policy. The policy officer is prompted to access a policy database and is instructed to download a new policy when the system has determined that a policy is ineffective and users are consistently out of compliance with the current policy. The new policy(s) are automatically added to the policy effectiveness system and the organization's policy manual.

Software resources include software listings and updates, guidelines for proper use including email etiquette, and netiquette training, Internet information and personal safety training, optional registration of an encryption private or public key with the system, a listing of the organization's approved and licensed software, software downloading guidelines and approved procedures, tech support for user's questions Registering newly downloaded software to the system, management approved trialware, shareware and others for review by the organization, operations and support information, regulation, policy, and Freedom of Information Act materials, information explaining how the system works including product support and services, telephony, text-based support, and in-house support options, a simple do & don't security module for non technical activity, and online safety information

Security, System Backup, and Recovery Processes

Users must present a password and hardware token to access the policy effectiveness system **100**. Most organizations concentrate their security resources on securing the perimeter of their network. Unfortunately, the greatest threat to an organization is its employees, who, with network access can cause greater damage than an external intruder.

The policy effectiveness system **100** employs an electronic tag to monitor document level access, security and to track information on a per document basis. This creates the opportunity to prove document authenticity, to track the copies and revisions of a document, and to monitor and report document access and disclosures.

System Backup and Recovery

The policy effectiveness system **100** has an online backup feature. This feature offers full redundancy, without the expense of off-site storage, and limits the process of physically cataloging and indexing backup tapes. Cataloging and indexing backups is automatically completed by the system. Backman is an existing software that does this.

Software Compliance

Most large organizations are not cognizant of the type of software licenses they have, which workstation and/or server has which software, who is using what software, and whether or not the organization is in compliance with their software licensing agreements. Users can easily download freeware, shareware trialware, and permware software from the Internet. All software is distributed with compliance conditions or restrictions of its use, even if it is identified as freeware, shareware and trialware, or is copyrighted but freely distributed.

To effectively monitor an organization's software compliance, periodic network audits are needed to identify deviations in the software inventory, and to reconcile software license agreements with software and hardware inventories. Products that monitor software licenses are known in the art, for example the FlexIM software by Globetrotter.

Each user is registered in the user profile database **150**. The user profile database **150** includes a user's hardware and software inventory information, as well as the user's name, user's email address, user's surface mail address, employment status (e.g., temp, contract, virtual), title, department, organizational chart indicating who the user reports to, the direct reports, his assistant, and mail station address. It also may indicate the software present on a user's workstation and the user's system access and security status.

The user profile database **150** also retain copies of any Employment Agreements and other employment-related contracts, maintains a record of the users' policy training and exam status, policy compliance history, network activity, and any special network access or privileges such as using the network for charitable use. Additionally, the user profiles **150** may also monitor software downloads from the network, or Internet, to hardware through network activity reports and network audits, including any software approved for use by management and other special approvals. Additional user information can be monitored and collected to assist the organization's reporting needs.

The policy effectiveness system **100** includes an object library/object level licensing system similar to FlexIM by Globetrotter.

The policy compliance monitor **110** features dynamic updating and exchanging of software licensing agreements. The compliance monitor **110** reviews all software license agreements and maintains records of the vendor information. The compliance monitor **110** sends a notification to the system administrator indicating that a software license is about to expire. The system administrator is prompted to send an email to the licensing organization to update the license agreement. Once the updated license agreement is received via email, the system automatically updates the software license registered and stored in the compliance monitor **110**.

The policy effectiveness module **120** monitors and tracks network activity including all hardware and software in the policy effectiveness system **100**. This module can generate reports to track an organization's user access including failed login attempts and all attempts to launch privileged applications, any changes to system configuration parameters software downloads from the Internet, software and hardware usage, location of software, location of software license agreements, type of software agreements, coordination of software license agreements with software utilization, statistical and graphical information regarding justification for software purchases, upgrades and maintenance expense, software installations, software compliance, appropriateness, inappropriateness and excessive use of software and hardware resources throughout the enterprise, the number of people waiting for access to software applications, access time, value of software being used at anytime, the need for upgrades, the need for training, projections for hardware, software and licensing costs/usage throughout the enterprise, hardware demand predictions, recommended re-route of software and hardware, personally installed or permitted software installation, need to streamline and more effectively use under utilized system resources, over utilization of system resources, potential policy infringements, system trends per department use, and the allocation of related costs related to department.

Software Applications Archive

The system records the storage location of all the software applications, software manuals, and software vendor infor-

mation used by the organization to create documents. In the event that records or documents, written in older versions of software, must be produced, the software will be preserved and available for use.

The foregoing description of the exemplary embodiments of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not with this detailed description, but rather by the claims appended hereto.

What is claimed is:

1. A method for dynamically assisting a system administrator of a computer network in upgrading compliance policy based on behavior of system users, the method comprising the steps of:

storing in a database a plurality of compliance policy options;

developing an initial compliance policy option potentially applicable to network users;

automatically evaluating over time the appropriateness of the initial compliance policy option based on the potentially evolving compliance history of users;

automatically compiling and providing to the system administrator over time a dynamic knowledge base comprising automated network user policy compliance violation documentation;

automatically determining from the knowledge base policy compliance violation documentation that the initial compliance policy option is ineffective;

automatically selecting from the database and recommending to the system administrator an alternate compliance policy option; and

automatically requesting that the system administrator confirm the change to the alternate compliance policy option,

whereby compliance policy options are dynamically altered and provided to the system administrator in order to eliminate ineffective compliance policy options.

2. The method of claim 1, further comprising the steps of:

electronically generating a network security policy compliance value based on monitoring network user compliance for a plurality of network users;

electronically comparing the compliance value to a target compliance value, wherein the target compliance value defines a baseline for network security compliance; and

undertaking a network policy compliance action based on a difference between the compliance value and the target compliance value.

3. The method of claim 2, wherein the compliance option is selected from a group comprising:

electronically implementing a different network security policy selected from network security policies stored in the database;

generating at least one policy effectiveness reports; and

providing a retaining module to network users.

4. The method of claim 1, further comprising the step of electronically undertaking a user compliance action in response to evaluating network users' compliance with a network security policy.

5. The method of claim 4, wherein the evaluating step comprises the steps of:

generating a network security policy compliance value based on monitoring network user compliance; and

comparing the compliance value to a target compliance value, wherein the target compliance value defines a baseline for network security policy compliance; and

wherein the undertaking step is based on a difference between the compliance value and the target compliance value.

6. The method of claim 5, wherein the user compliance option is selected from a group comprising:

notifying a network user;

notifying a policy administrator;

providing a retraining module to the network user; and

restricting the network user's network access rights.

7. The method of claim 3, wherein at least one network security policy has a security level identifier identifying the relative restrictiveness of the policy, wherein the implementing step includes the step of electronically selecting a network security policy based on the security level identifier.

8. The method of claim 1, further comprising the step of interactively generating a network security policy, the generating step comprising the steps of:

electronically providing a suggested network security policy to a plurality of network users;

electronically receiving a modified network security policy from at least one of the network users;

electronically providing at least one of the modified policies to the network users; and

receiving a group modified policy from the network users.

9. The method of claim 1, further comprising the steps of:

electronically monitoring network user compliance with the compliance policy, including the steps of:

electronically providing a network policy exam to a network user;

electronically receiving exam answers from the network user;

electronically evaluating the exam results to generate an evaluation score;

notifying the network user of the evaluation score; and

storing the evaluation score in a database.

10. The method of claim 1, wherein the compliance policy comprises:

a network hardware policy;

an email policy;

an internet policy;

a software license policy;

a document management system policy; and

a network security enforcement policy.

11. An apparatus for dynamically assisting a system administrator of a computer network in upgrading compliance policy based on behavior of system users, the apparatus comprising:

a computer system comprising at least one processor and at least one memory, the computer system being adapted and arranged for:

storing in a database a plurality of compliance policy options;

developing an initial compliance policy option potentially applicable to network users;

automatically evaluating over time the appropriateness of the initial compliance policy option based on the potentially evolving compliance history of users;

automatically compiling and providing to the system administrator over time a dynamic knowledge base comprising automated network user policy compliance violation documentation;

automatically determining from the knowledge base policy compliance violation documentation that the initial compliance policy option is ineffective;

automatically selecting from the database and recommending to the system administrator an alternate compliance policy option; and

automatically requesting that the system administrator confirm the change to the alternate compliance policy option,

whereby compliance policy options are dynamically altered and provided to the system administrator in order to eliminate ineffective compliance policy options.

12. An article of manufacture for dynamically assisting a system administrator of a computer network in upgrading compliance policy based on behavior of system users, the article of manufacture comprising a computer-readable storage medium having a computer program embodied therein that causes the computer network to perform the steps of:

storing in a database a plurality of compliance policy options;

developing an initial compliance policy option potentially applicable to network users;

automatically evaluating over time the appropriateness of the initial compliance policy option based on the potentially evolving compliance history of users;

automatically compiling and providing to the system administrator over time a dynamic knowledge base comprising automated network user policy compliance violation documentation;

automatically determining from the knowledge base policy compliance violation documentation that the initial compliance policy option is ineffective;

automatically selecting from the database and recommending to the system administrator an alternate compliance policy option; and

automatically requesting that the system administrator confirm the chance to the alternate compliance policy option,

whereby compliance policy options are dynamically altered and provided to the system administrator in order to eliminate ineffective compliance policy options.

* * * * *